2014-15 ANNUAL REPORT

Office of the Information and Privacy Commissioner of Alberta

Office of the Information and
Privacy Commissioner of Alberta

Office of the Information and
Privacy Commissioner of Alberta
410, 9925 - 109 Street, NW
Edmonton, AB T5K 2J8

NOVEMBER 2015

Phone: 780.422.6860
Toll Free: 1.888.878.4044
Fax: 780.422.5682
Email: generalinfo@oipc.ab.ca

www.oipc.ab.ca

Office of the Information and
Privacy Commissioner of Alberta

November 2015

The Honourable Robert E. Wanner
Speaker of the Legislative Assembly
325 Legislature Building
10800 - 97 Avenue
Edmonton, AB T5K 2B6

Dear Mr. Speaker:

I am honoured to present to the Legislative Assembly the Annual Report of the Office of the Information and Privacy Commissioner for the period April 1, 2014 to March 31, 2015.

This report is provided in accordance with section 63(1) of the *Freedom of Information and Protection of Privacy Act*, section 95(1) of the *Health Information Act*, and section 44(1) of the *Personal Information Protection Act*.

Yours truly,

Original signed by
Jill Clayton
Information and Privacy Commissioner

Table of Contents

Commissioner's Message 6

About the Office 9
Mandate 10
OIPC Organizational Structure 2014-15 12
The Process: Request for Review/Complaint 13
OIPC as a Public Body 14
Financial Overview 16

Trends and Issues 17
Legislative Reform 18
Mandatory Breach Reporting 19
Delays and Challenges to the OIPC 20
National Security and Information Sharing 21
Right to be Forgotten 22

By the Numbers 25
Graph A: Total Cases Opened 27
Graph B: Total Cases Closed 27
Table 1: Cases Opened by Case Type 28
Table 2: Cases Closed by Case Type 29
Table 3: Percentage of Cases Closed by Resolution Method 30
Graph C: Percentage of Cases Closed by Resolution Method 31
Table 4: Telephone Calls, Emails And Written Enquiries 31

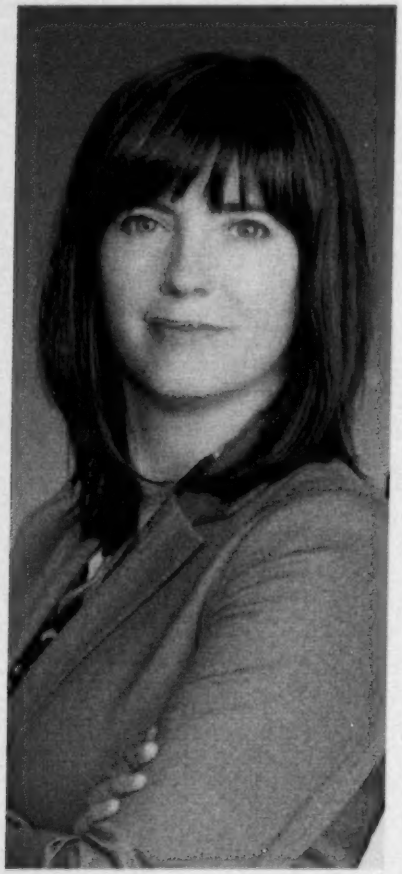
Regulation and Enforcement 33
Request for Time Extensions Under FOIP 34
Privacy Impact Assessment Reviews 35
Investigation Reports 36
Privacy Breach Reporting under HIA 37
Privacy Breach Reporting under FOIP 37
Mandatory Breach Reporting Under PIPA 38
Offence Investigations 40
Summary of Significant Decisions 40
Judicial Reviews and Other Court Decisions 42

Education and Outreach 49
Presentations, Forums and Workshops 50
Collaboration with Other Jurisdictions 51
Independent Research 52
Media Requests 53
Robert C. Clark Award 53

Financial Statements 55

Appendices 67
Appendix A: Cases Opened Under FOIP, HIA, PIPA by Entity Type 68
Appendix B: Cases Closed Under FOIP, HIA, PIPA by Entity Type 71
Appendix C: Orders, Decisions and Public Investigation Reports Issued 74
Appendix D: Accepted Privacy Impact Assessments by Public Body, Custodian and Organization Types 76

Commissioner's Message



As described in last year's Annual Report, at the end of the last fiscal year (2013-14) the Office of the Information and Privacy Commissioner had just implemented a new office structure. The new structure is a significant change from what was previously in place, and was designed to position the office to be more responsive to a changing environment. Instead of three operational teams dealing independently with issues arising under the *Freedom of Information and Protection of Privacy Act* (the FOIP Act), the *Health Information Act* (HIA) and the *Personal Information Protection Act* (PIPA), the new structure is based on function:

- The Compliance and Special Investigations team deals with self-reported breaches, Commissioner-initiated investigations, offence investigations, and privacy impact assessment reviews – regardless of whether these matters arise under the FOIP Act, PIPA, or the HIA.
- The Mediation and Investigation team works to resolve complaints and requests for review; again, regardless of which Act applies.
- The newly established Intake and Case Review unit merges what was previously two independent intake functions (divided geographically: Calgary and Edmonton) into one.

After implementing these changes in January 2014, the real work continued throughout fiscal year 2014-15 to entrench the new structure and identify opportunities to improve our efficiency and effectiveness by consolidating processes, reducing inconsistencies and communicating changes to the public and our regulated stakeholders.

We started somewhat behind the eight-ball, with a backlog of complaints that had been placed in abeyance in 2013-14 while we prioritized time-sensitive matters, such as requests for review, and worked to fill staff vacancies. Once the new office structure and staff were in place, dealing with the backlog was a priority. A process to triage complaints that had been held in abeyance was implemented, with an eye to identifying and quickly resolving those that did not require lengthy investigation.

This process was successful and, in the initial stages, 60–65% of cases funneled through triage were resolved as a result. Mid-way through fiscal year 2014-15 we were no longer placing any cases in abeyance. The complaints triage process has now been made permanent, and continues to resolve over 50% of complaints channeled through this route. The average time for files that are resolved in this process is 15 business days from the date the triage manager evaluates the file.

Additional process changes introduced in November 2014 include: requesting copies of records at issue immediately after a case is opened, rather than after the case is assigned, and exploring information mapping formats to expedite letters of finding and enhance consistency and readability. In January 2015 we rolled out a new case management system which will further enhance the office's ability to track and report on files, analyze processes, and identify opportunities for improvement. For four months, we were also able to bring in experienced contract staff on a part-time basis to help with the backlog.

At the same time we were making these and other internal adjustments to improve the effectiveness, efficiency and timeliness of our processes, we found our external environment was changing. Going back a few years, but gaining momentum in 2014-15, we encountered the following: (1) public bodies missing OIPC-set deadlines to respond to questions/make submissions on the issues, and (2) public bodies claiming "privilege" as a reason to refuse to provide records to my office.

We recognize that resourcing may be a factor affecting public bodies' ability to meet deadlines; however, every extension of a deadline delays the resolution of a matter. The OIPC is reluctant to decide cases without having the benefit of all relevant information. Nevertheless, in some instances we have found it necessary to conclude cases based on the limited information provided.

With respect to claims of privilege, many readers of this Annual Report will be aware of the Alberta Court of Appeal's decision in *University of Calgary v. JR*, 2015 ABCA 118 (available on www.canlii.org). In that case, the Court decided that I cannot compel records that are alleged to be subject to solicitor-client privilege. However, I note that, until the Court's decision was issued in early April 2015, the law in Alberta was that I did have the ability to compel production of these records. More importantly, the power to compel had almost never been used as the records were provided voluntarily to my office as part of the mediation process, or at a formal quasi-judicial inquiry. For some reason, this practice changed, and public bodies — particularly provincial government public bodies — have been increasingly refusing to provide these records since 2013-14.

I have applied for leave to appeal the Court of Appeal's decision to the Supreme Court of Canada. However, at this time, it remains the case that approximately 80 FOIP and PIPA cases before the office involve issues related to claims of privilege. It is expected that my ability to resolve these cases, and the timeline to resolve them, will be impeded by the Court of Appeal decision.

I would like to end this message by expressing my deep appreciation to my colleagues at the OIPC for their work over this past year. Albertans are well-served by your diligence and commitment to access to information and protection of privacy.

Jill Clayton
Information and Privacy Commissioner

In 2014-15, the OIPC closed:

1311 files overall*: a **13**% increase from 2013-14

273 complaint files: a **100**% increase from 2013-14

*not including intake files

About the Office

Mandate

The Information and Privacy Commissioner is an Officer of the Legislature. The Commissioner reports directly to the Legislative Assembly of Alberta and is independent of the government of the day.

Through the Office of the Information and Privacy Commissioner (OIPC), the Commissioner performs the legislative and regulatory responsibilities set out in Alberta's three access and privacy Acts.

Freedom of Information and Protection of Privacy Act

The *Freedom of Information and Protection of Privacy Act* (FOIP or the FOIP Act) applies to 1,160 public bodies, including provincial government departments and agencies, boards and commissions, municipalities, Métis settlements, drainage districts, irrigation districts, housing management bodies, school boards, post-secondary institutions, public libraries, police services, police commissions and health authorities.

The FOIP Act provides a right of access to any record in the custody or under the control of a public body, subject to limited and specific exceptions. The Act also gives individuals the right to access their own personal information held by public bodies and to request corrections to their own personal information. The Act protects privacy by setting out the circumstances in which a public body may collect, use, or disclose personal information.

Health Information Act

The *Health Information Act* (HIA) applies to more than 54,900 health custodians, including Alberta Health, Alberta Health Services, Covenant Health, nursing homes, physicians, registered nurses, pharmacists, optometrists, opticians, chiropractors, podiatrists, midwives, dentists, denturists, and dental hygienists.

HIA also applies to "affiliates," who perform a service for custodians, such as employees, contractors, students and volunteers. Custodians are responsible for the information collected, used and disclosed by their affiliates.

HIA allows health services providers to exchange health information to provide care and to manage the health system.

The Act protects patients' privacy by regulating how health information may be collected, used and disclosed and by establishing the duty for custodians to take reasonable steps to protect the confidentiality and security of health information. The Act also gives individuals the right to access their own health information, to request corrections, and to have custodians consider their wishes regarding how much of their health information is disclosed or made accessible through Alberta's provincial electronic health record system (i.e. Alberta Netcare).

Personal Information Protection Act

The *Personal Information Protection Act* (PIPA) applies to provincially-regulated private sector organizations, including businesses, corporations, associations, trade unions, private schools, private colleges, partnerships, professional regulatory organizations, and any individual acting in a commercial capacity.

PIPA protects the privacy of clients, customers, employees and volunteers by establishing the rules for the collection, use and disclosure of personal information by organizations.

The Act seeks to balance the right of the individual to have his or her personal information protected with the need of organizations to collect, use or disclose personal information for reasonable purposes. PIPA also gives individuals the right to access their own personal information held by organizations and to request corrections.

The Commissioner oversees and enforces the administration of these Acts to ensure their purposes are achieved.

The Commissioner's powers, duties and functions include:

- providing independent review and resolution on requests for review of responses to access to information requests and complaints related to the collection, use and disclosure of personal and health information
- investigating any matters relating to the application of the Acts, whether or not a review is requested
- conducting inquiries to decide questions of fact and law and issuing binding orders
- educating the public about the Acts, their rights under the Acts and access and privacy issues in general
- receiving comments from the public concerning the administration of the Acts
- giving advice and recommendations of general application respecting the rights or obligations of stakeholders under the Acts
- engaging in or commissioning research into any matter affecting the achievement of the purposes of the Acts
- commenting on the implications for access to information or for protection of personal privacy of proposed legislative schemes and existing or proposed programs
- commenting on the access and privacy implications of privacy impact assessments submitted to the Commissioner
- commenting on the privacy and security implications of using or disclosing personal and health information for record linkages or for the purpose of performing data matching

Vision

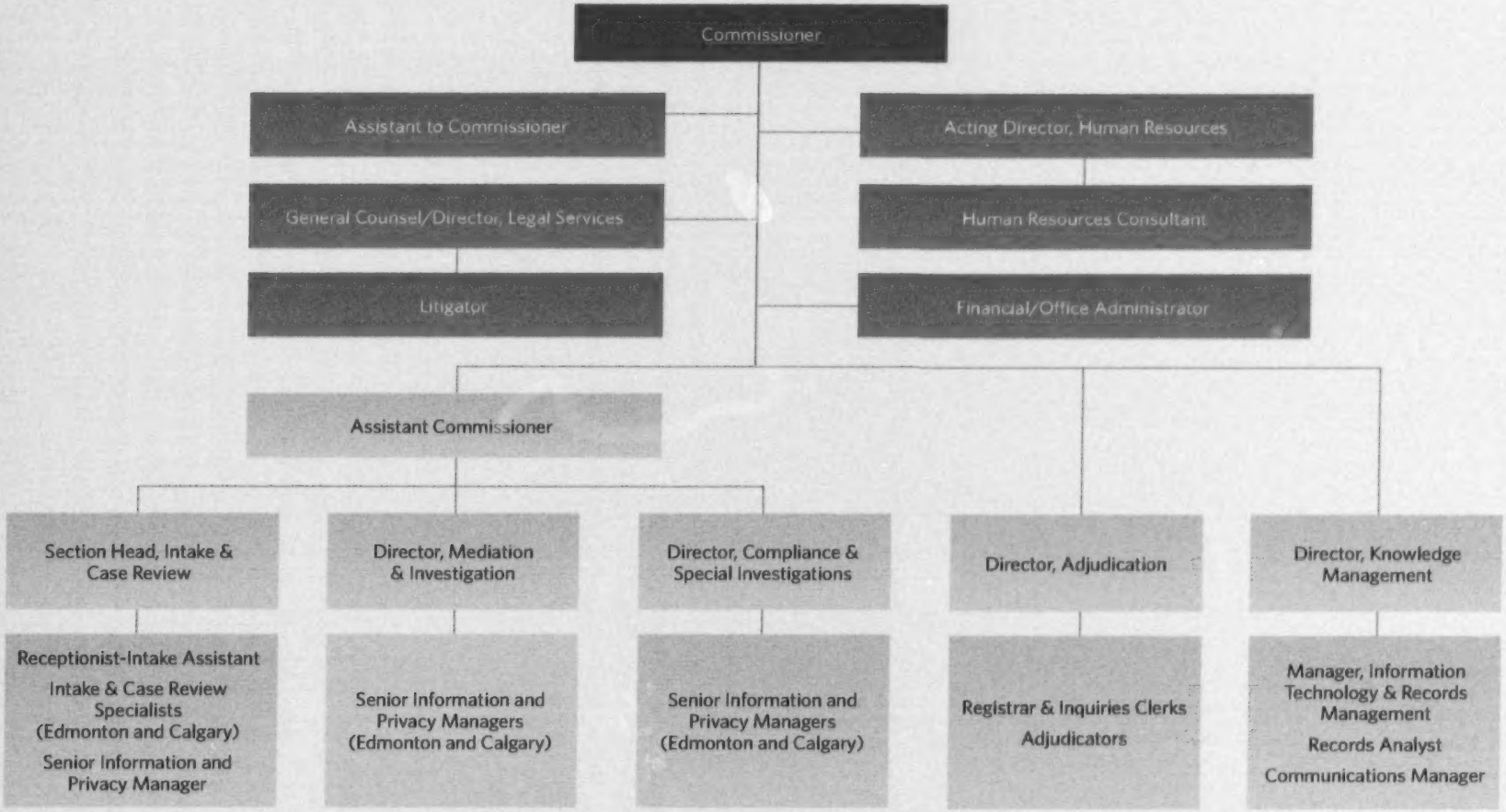
A society that values and respects access to information and personal privacy.

Mission

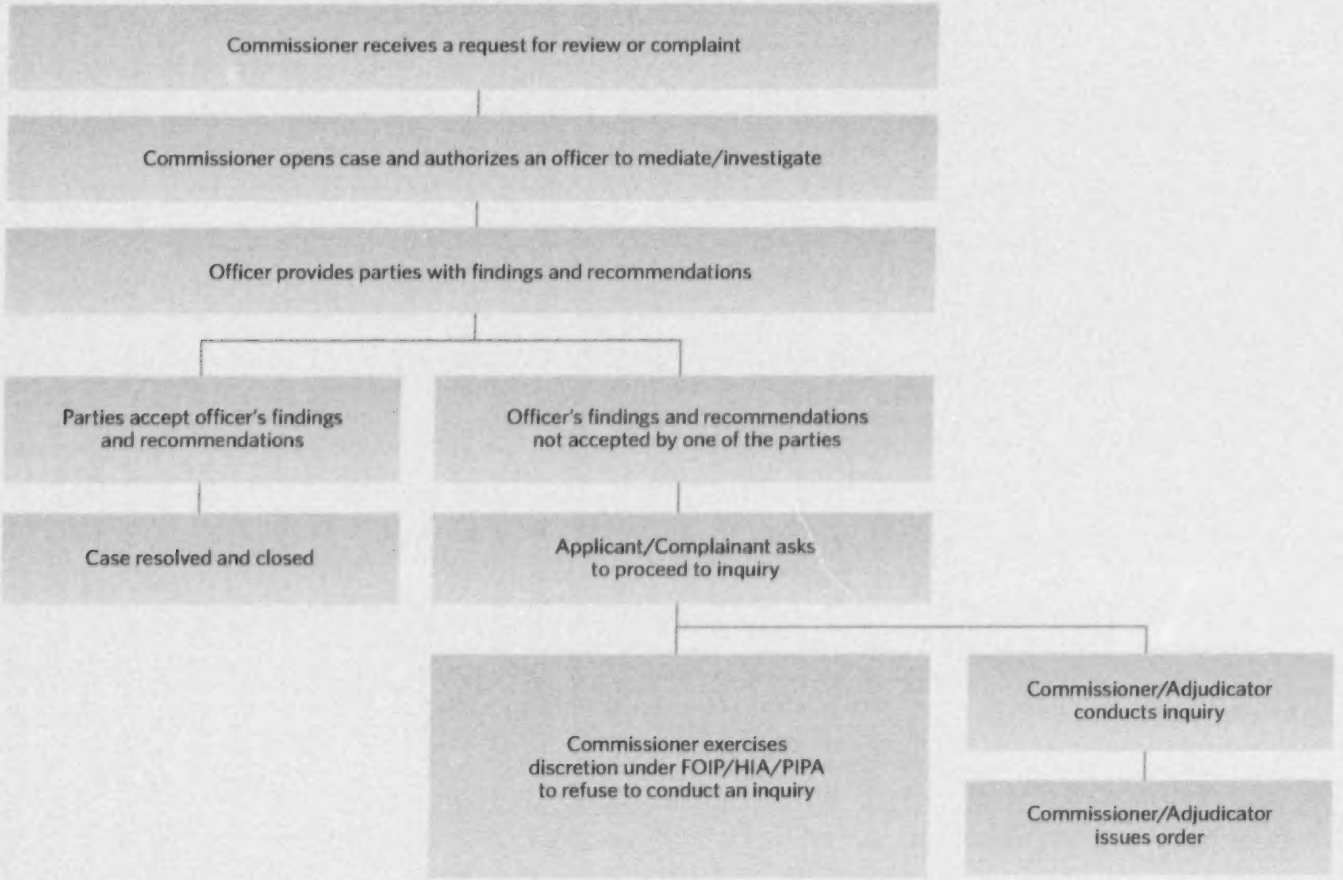
Our work toward supporting our vision includes:

- advocating for the privacy and access rights of Albertans
- ensuring public bodies, health custodians and private sector organizations uphold the access and privacy rights contained in the laws of Alberta
- providing fair, independent and impartial reviews in a timely and efficient manner

OIPC Organizational Structure 2014-15



The Process: Request for Review/Complaint


Commissioner receives a request for review or complaint
Commissioner opens case and authorizes an officer to mediate/investigate
Officer provides parties with findings and recommendations
Parties accept officer's findings and recommendations
Officer's findings and recommendations not accepted by one of the parties
Case resolved and closed
Applicant/Complainant asks to proceed to inquiry
Commissioner exercises discretion under FOIP/HIA/PIPA to refuse to conduct an inquiry
Commissioner/Adjudicator conducts inquiry
Commissioner/Adjudicator issues order

OIPC as a Public Body

FOIP Requests to OIPC

Section 4(1)(d) of the FOIP Act states that records created by or for or in the custody or under the control of the Commissioner in the exercise of her legislative functions are excluded from the application of the FOIP Act.

In 2014-15, the OIPC received one personal information request pursuant to the FOIP Act and five informal requests for information. OIPC responded to all the requests.

With respect to the one personal information request made under the FOIP Act, the applicant was informed that the applicant had not provided enough detail to enable the OIPC to identify the records requested. The applicant was also informed that records related to the Commissioner's legislative functions were excluded from the scope of the FOIP Act under section 4(1)(d).

On October 30, 2014, the OIPC received written notification from the Minister of Service Alberta that the applicant had requested a review of the OIPC's response to the personal information request.

Under section 77(2) of the FOIP Act, a person who makes a request to the Commissioner for access to a record may ask an adjudicator to review any decision, act or failure to act of the Commissioner that relates to the request. To ask for a review, an applicant must make a written request to the Minister of Service Alberta within 60 days of the applicant receiving the Commissioner's decision on the applicant's access request (sections 79(1) and 79(2)(a)(i)). Upon receipt of a request for review, the Minister must as soon as practicable give the request to an adjudicator (section 80). Section 75(1) states that the Lieutenant Governor in Council may designate a judge of the Court of Queen's Bench of Alberta to act as an adjudicator.

An adjudicator was designated March 19, 2015. This matter is still outstanding at the end of 2014-15 fiscal year, along with another request for review that was reported in the 2013-14 Annual Report.

OIPC Privacy Matters

In 2014-15, the OIPC conducted four internal investigations into potential privacy breaches:

- Two incidents involved OIPC sending correspondence to incorrect public bodies. Both incidents were the result of human errors and staff members were reminded of their obligations to double-check for the correct public bodies prior to sending correspondence. In both incidents, the disclosures presented no real risk of significant harm to the individuals involved. All parties were notified of the incidents and the correspondence was retrieved.
- The OIPC sent correspondence to an individual that had been authorized to provide FOIP services on behalf of a public body. The public body had not notified the OIPC that the individual was no longer its FOIP contact. The OIPC asked the public body to update its FOIP contact information. The disclosure was limited to the names of individuals in their official capacity.
- An internal email containing personal information about a contractor was sent to the wrong OIPC staff member. The sender had not noticed the system had selected the wrong staff member. The staff member confirmed receipt of the email, knew that it did not pertain to any matter the staff member was dealing with, and deleted the email. The sender is mindful of the need to check the recipient selected before sending future emails. The affected contractor was notified of the incident.

The OIPC also conducted a penetration test on its IT infrastructure, a physical security assessment of the OIPC's Edmonton office, and a social engineering (phishing) attack test on OIPC employees. The main objectives of the tests were to verify if existing technical, physical and administrative security controls were working as intended and to identify areas of improvement. These tests were part of the OIPC's ongoing initiative to "walk the talk," by ensuring appropriate steps are taken to protect OIPC information assets.

Existing physical access controls prevented the office space and server room from being compromised during the test. Also, within the test parameters, the OIPC's IT infrastructure could not be compromised from the Internet - no external exploitable vulnerabilities were identified. The test identified some internal network exploitable vulnerabilities, which are being addressed. The test confirmed an external vulnerability on the third party IT infrastructure that hosted the OIPC's website. The website does not collect personal information other than what is necessary to operate the site. Steps were taken to move the site to a more secure environment managed by a different vendor.

Employees of the OIPC were subjected to a social engineering (phishing) test. The sophisticated phishing campaign was designed with the help of the OIPC to take into account that OIPC employees would generally have a greater awareness of privacy and security. The test, which was intended to solicit and obtain usernames and passwords, was very successful. This simply showed that no one is immune to social engineering attacks, including subject matter experts. The event concluded with a staff education session.

Proactive Travel and Expenses Disclosure

The OIPC continues to publicly disclose the vehicle, travel and hosting expenses of the Commissioner, and the travel and hosting expenses of the Assistant Commissioner and OIPC Directors on a bi-monthly basis.

Financial Overview

For the 2014-15 fiscal year, the total approved budget for the OIPC was $6,983,000. The total cost of operating expenses and capital purchases was $6.8 million. The OIPC returned $193,887 (2.8% of the total approved budget) to the Legislative Assembly.

Total Actual Costs Compared to Budget

	VOTED BUDGET	ACTUAL	DIFFERENCE
Operating Expenses*	$ 6,983,000	$ 6,770,462	$ 212,538
Capital Purchases	0	18,651	(18,651)
Total	**$ 6,983,000**	**$ 6,789,113**	**$ 193,887**

*Amortization is not included

Salaries, wages, and employee benefits make up approximately 82.5% of the OIPC's operating expenses budget. Payroll related costs were $574,131 below budget due to: vacant positions, staff leaves, new staff hired at lower salaries than estimated, and lower professional and conference fees due to vacancies.

Reduced payroll and benefits costs were offset by increased costs for supplies and services, which were $361,593 over budget and comprised of: approximately $100,000 for contracted legal services (due to OIPCs Litigator being on leave); $105,000 for contracted office administration and finance services not budgeted for; $228,000 for contracted services to fulfill the office mandate including research for HIA and PIPA review submissions, PIA reviews and complaint investigations, external adjudication due to commissioner conflict, and an independent review of adjudicator's position classification. Various other supplies and services were under budget a net of approximately $71,000.

Total Actual Costs Compared to Prior Year

	2014-15	2013-14	DIFFERENCE
Operating Expenses	$ 6,770,462	$ 6,075,438	$ 695,024
Capital Purchases	18,651	148,193	(129,542)
Total	**$ 6,789,113**	**$ 6,223,631**	**$ 565,482**

Total costs for operating expenses and equipment purchases increased by $565,482 from the prior year. This is due primarily to having 39 full time employees throughout the 2014-15 fiscal year, whereas the prior year was understaffed by 10 positions for approximately 6 months.

Trends & Issues

This section of the Annual Report, first introduced in 2012-13, is intended to provide some context for the work of the OIPC by highlighting some of the provincial, national and international issues and trends that shape and influence the access and privacy landscape, and characterize the fiscal year.

Legislative Reform

Fiscal year 2014-15 saw important amendments to PIPA and HIA as a result of issues that arose in 2013-14.

PIPA Constitutional Amendment

In November 2013, the Supreme Court of Canada released its decision in *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401,* (2013 SCC 62), ruling that Alberta's PIPA is unconstitutional and declaring it invalid. The Court gave the Alberta Legislature 12 months to bring the Act in line with the *Canadian Charter of Rights and Freedoms.*

After the Court granted a six month time extension, the government introduced Bill 3, the *Personal Information Protection Amendment Act, 2014,* in the Legislature on November 18, 2014. The proposed amendments would add to PIPA an exception to consent for the collection, use and disclosure of personal information by a trade union in limited circumstances relating to a labour relations dispute. This is similar to a solution recommended by the Commissioner in a letter to the government in December 2013.

The amendments were passed and came into force December 17, 2014.

Breach reporting and notification in the health sector

As reported in the 2013-14 Annual Report, the Medicentres Canada Inc. incident, involving the theft of an unencrypted laptop containing billing information for over 600,000 Albertans, served to draw attention to the importance of including privacy breach reporting and notification requirements in access and privacy legislation.

The incident led to the Commissioner writing to the Minister of Health, in February 2014, to formally request the Government of Alberta consider amending Alberta's *Health Information Act* (HIA) to include mandatory breach reporting and notification provisions.

In May 2014, the government introduced breach notification amendments to HIA (Bill 12, *Statutes Amendment Act, 2014*). These amendments include mandatory notification:

- by an affiliate to a custodian of a loss or unauthorized access to or disclosure of individually identifying health information in the custody or control of the custodian, and
- by a custodian to the Commissioner, the Minister of Health and individuals who are the subject of the information, when there is a risk of harm to an individual as a result of the loss or unauthorized access or disclosure. (An exception to notifying individuals exists where notification could result in a risk of harm to their mental or physical health.)

Amendments would also expand the Commissioner's ability to disclose information by allowing the Commissioner to disclose information:

- to any person where the Commissioner reasonably believes the disclosure is necessary to protect the privacy, health or safety of an individual, or is in the public interest, and
- to the Minister of Health where the Commissioner is of the opinion that the disclosure is necessary to enable the Minister to exercise his or her powers or carry out his or her ministerial duties or functions.

The amendments passed, with the breach notification amendments coming into force on proclamation, and the provision allowing disclosure by the Commissioner coming into force June 17, 2014.

Mandatory Breach Reporting

One trend that 2014-15 should be noted for is the amount of attention privacy breaches received, provincially, nationally and internationally. In Alberta, the OIPC saw a significant increase in the number of self-reported breaches. Public bodies under FOIP reported 41 breaches to the OIPC, up from 22 the previous year – an increase of 86%. The number of breaches self-reported by custodians under the HIA also increased by 12% (from 68 to 76), as did the number of breaches reported by organizations subject to PIPA (a 44% increase, from 96 to 138).

Almost every week saw a new report of another incident, whether it was a compromised payment system at Home Depot (over 97,000 Albertans affected), a cyberattack against eBay Inc. (11.4 million active and inactive accounts in Canada), or health workers snooping the medical records of the (now former) Mayor of Toronto.

This last event, coupled with other high-profile health information snooping cases in Ontario, led to calls for legislative changes to require that such incidents be reported to Ontario's Information and Privacy Commissioner[1].

Federally, the government introduced Bill S-4 in April 2014, which included proposed amendments to the *Personal Information Protection and Electronic Documents Act* (PIPEDA) for mandatory breach notification provisions similar to those found in Alberta's PIPA[2]. S-4 provisions require organizations to notify affected individuals and the federal Privacy Commissioner of a breach of security safeguards, where the breach poses a real risk of significant harm to affected individuals. Organizations are also required to keep a record of data breaches, including those that do not meet the harm threshold, and report all breaches to the Commissioner upon request. Knowingly failing to report or record a breach is an offence subject to fines of up to $100,000.

In British Columbia, the Special Committee reviewing PIPA tabled its report in February 2015. The Committee made 15 recommendations, including mandatory breach notification to individuals and reporting of incidents to the BC Information and Privacy Commissioner. The Committee recommended that the proposed threshold to trigger breach reporting and notification in BC's PIPA be the same as that in Alberta's PIPA: an organization should be required to notify the Commissioner and affected individuals of any breach involving personal information under its control if it is reasonable in the circumstances to believe that the breach could create a real risk of significant harm to an individual. The Committee said this threshold "achieves the right balance in the appropriate level of risk to trigger notification requirements and is in harmony with the Alberta and proposed federal models."

As previously noted, amendments to Alberta's HIA to include mandatory breach reporting and notification received Royal Assent in May 2014, but have yet to be proclaimed in force. The threshold for notifying individuals, the Commissioner, and the Minister of Health about an incident is where there is a 'risk of harm' to an individual. This is a different threshold from that set out in Alberta's PIPA.

In 2014-15, the OIPC opened 255 self-reported breach cases, a 37% increase from 2013-14.

FOIP **86**% increase (41 cases)

HIA **12**% increase (76 cases)

PIPA **44**% increase (138 cases)

[1] Bill 119, which seeks to amend Ontario's *Personal Health Information Protection Act, 2015*, was tabled in September 2015 and includes mandatory breach reporting, as well as provisions to make it easier to prosecute offences, and increased fines.

[2] Bill S-4, the *Digital Privacy Act*, received Royal Assent on June 18, 2015. However, provisions related to mandatory breach notification do not come into force until regulations have been enacted.

Delays and Challenges to the OIPC

One of the more concerning trends that rose to the fore in 2014-15 has been the increasing number of challenges the OIPC has experienced in attempting to investigate, mediate and settle requests for review, and complete inquiries. These challenges lead to delays, increased costs for all parties, and frustrate timely access to information and effective oversight of compliance with Alberta's access and privacy laws. Two case examples serve to illustrate this point: (1) the investigation initiated by the Commissioner of Medicentres Canada Inc. (Medicentres), and (2) the investigation initiated by the Commissioner into the Government of Alberta's processing of access to information requests under FOIP.

Medicentres Canada Inc.

In the first example, following the theft of a laptop computer owned by an information technology consultant who was performing services for Medicentres, the Commissioner initiated an investigation of the incident.

In July 2014, during the investigation, Medicentres brought an application for judicial review, seeking a prohibition order to prohibit the Commissioner from concluding the investigation and, on the ground of procedural unfairness, to prohibit the Commissioner from publishing any report of the investigation that included any references to certain emails; any comment or statement that Medicentres had authority from physicians to provide information in response to the investigation; and any comment, finding or recommendations about the loss of the laptop. Medicentres also asked for an interim order staying the investigation until the judicial review could be heard, and a publication ban on the investigation report pending the application for prohibition.

Although the Court ultimately dismissed Medicentres' application, the proceedings delayed the investigation and publication of the investigation report of the incident. Medicentres' application in this case is the first time such a proceeding has been initiated during an investigation initiated by the Commissioner.

Investigation into the Government of Alberta's processing of FOIP Requests

Another example of challenges leading to delay is the Government of Alberta's response to the investigation initiated by the Commissioner into how the government responds to requests for access to information.

The investigation was announced in May 2014 after discussions at the Alberta Legislature alleged political interference in the processing of access requests, and following the Commissioner's receipt of letters from the NDP Opposition (at the time) and the Canadian Taxpayers Federation asking for an investigation into delays in the release of records.

As part of the investigation, the OIPC requested documents from several Government of Alberta ministries. However, the information provided was redacted, sometimes quite heavily redacted, with no substantiation other than an assertion of "privilege". The Commissioner issued Notices to Produce Records to 13 Government ministries, including Executive Council (the Premier's Office) and Alberta Justice and Solicitor General. The Government responded by bringing a judicial review application for all 13 ministries. The matter has been set down to be heard by the court in February 2016, some 21 months from the initiation of the investigation.

Shortly after the Government brought its judicial review application, Alberta's Court of Appeal issued its decision in *University of Calgary v. JR* (2015 ABCA 118), overturning a 2013 decision of the lower court and finding the Commissioner does not have the power to compel production of records subject to solicitor-client privilege. The Commissioner is seeking leave to appeal this case to the Supreme Court of Canada.

At this time, however, in addition to *University of Calgary v. JR* and the Commissioner's investigation of how Government responds to requests for access, there are currently eight other cases involving solicitor-client and other legal privileges that are the subject of judicial review applications, in addition to a number of cases currently at mediation/ investigation and inquiry. The judicial review applications were brought by various Government ministries (three by Alberta Justice, and one by Alberta Health) – as well as three by police services, and one by an organization subject to PIPA. It is worth noting that six of these eight judicial review applications were brought before Alberta's Court of Appeal issued its decision in *University of Calgary v. JR*, the earliest having been filed on October 25, 2011.

National Security and Information Sharing

In the fall of 2014, following the tragic murders of Warrant Officer Patrice Vincent and Corporal Nathan Cirillo, in Saint-Jean-sur-Richelieu, Quebec and Ottawa, Ontario respectively, Canada's Information and Privacy Commissioners met in Ottawa and issued a Statement on National Security and Law Enforcement Measures. The Commissioners expressed condolences to the grieving families and friends of the victims, and at the same time noted the importance of critically determining any future course of action to ensure Canada remains safe, while ensuring Canadians' fundamental rights and freedoms are upheld. The Commissioners' Statement acknowledged that security is essential to maintaining democratic rights, but also noted that any response to such tragic events must be measured and proportionate, preserving democratic values.

In the Statement, Canada's Information and Privacy Commissioners called on the federal government to:

(1) adopt an evidence-based approach when considering new legislative proposals granting additional powers for intelligence and law enforcement agencies,

(2) engage Canadians in an open and transparent dialogue on whether new measures are required, and if so, on their nature, scope, and impact on rights and freedoms, and

(3) ensure that effective oversight be included in any legislation establishing additional powers for intelligence and law enforcement agencies.

In January 2015, the federal government introduced Bill C-51, the *Anti-terrorism Act, 2015* – legislation that raised concerns about the protection of civil liberties, freedom of speech, and privacy. Along with many other individuals and groups, Canada's Information and Privacy Commissioners jointly wrote to the Standing Committee on Public Safety and National Security to express deep concerns about the far-reaching implications of the Bill. In particular, the Commissioners focused on the Bill's "mandate for overbroad, unregulated and intrusive sharing of the personal information of ordinary Canadians" which would "facilitate a substantial shift towards routine surveillance of large portions of the populace."

The Commissioners made a number of recommendations for amendment to the Committee, focusing on the Bill's broad new information-sharing powers, and including but not limited to:

- Limiting information sharing to that which is strictly necessary to accomplish a specific security purpose associated with preventing "terrorist activity" or "threats to the security of Canada".

- Requiring all disclosing and recipient institutions to implement responsible information sharing practices and ensure that information sharing is conducted in a proportionate, transparent and accountable manner. These should be set out in binding regulations, and include limited retention periods, secure destruction of records when no longer required, and maintaining records reflecting what information was shared with whom, when, why and subject to what controls.
- Repealing sections of the Bill which would lead to recipient institutions using and further disclosing personal information to "any person" and for "any purpose".
- Restricting identified recipient institutions to those that have primary responsibility for law enforcement or national security.
- Introducing legislation to ensure that all national security and intelligence agencies are subject to meaningful, independent oversight and review.

Bill C-51 was eventually passed in the Senate in June 2015, without significant amendment. It is now being challenged in court on the basis that it is unconstitutional.

In January 2015, on Data Privacy Day, the Office of the Information and Privacy Commissioner of Alberta issued an independent research paper commissioned to provide a privacy perspective on multi-stakeholder government information sharing projects.

The paper, entitled *Government Information Sharing: Is Data Going Out of the Silos, Into the Mines?*, provides an overview of government information sharing projects across Canada and internationally, potential frameworks for analysis, citizen expectations, and an examination of actions taken to protect privacy. Looking at information sharing initiatives in Canada, Australia, the United States, United Kingdom and Denmark, the paper provides a critical look at a variety of projects, the concept of big data, the transparency or lack thereof of projects, and citizen reactions to different projects.

The paper concludes with an analysis of the risks involved in information sharing projects and proposals, including but not limited to establishing legal authority, security management, organizational commitment to privacy, and public relations and communications.

Right to be Forgotten

One of the most discussed issues in the access and privacy world of 2014-15 was a May 2014 decision of the Court of Justice of the European Union (ECJ) which highlighted the struggle between free speech and the protection of privacy.

The case arose after a Spanish man objected to the fact that Google searches on his name resulted in links to a 1998 newspaper article about the repossession of his home. In its decision, the Court ruled that citizens have a right to request their data be deleted from search results, finding that the rights of people whose privacy has been infringed outweighed the general public interest, although in certain cases the public interest will prevail. The decision does not mandate the permanent deletion of articles; instead, articles would not turn up in search results.

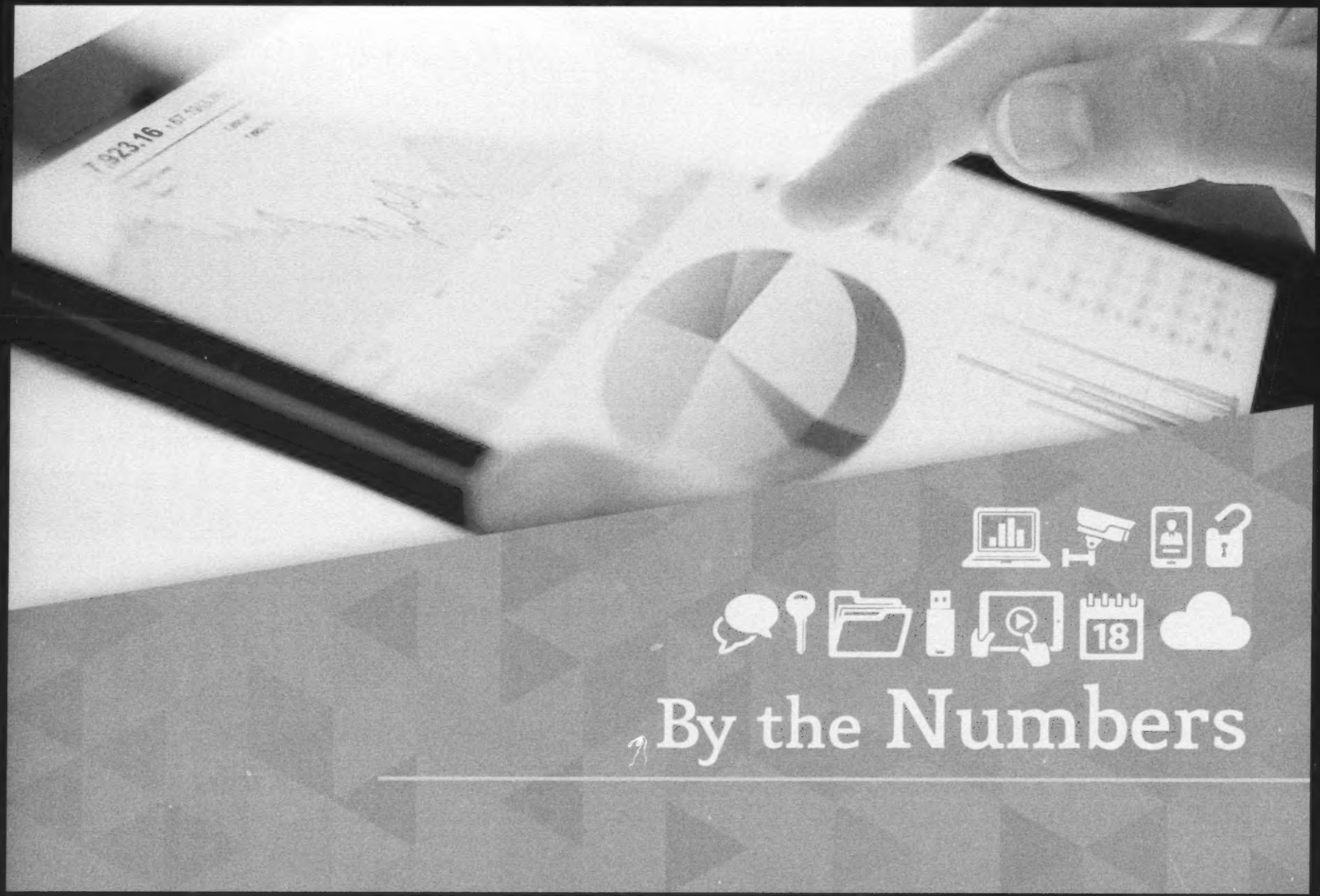
Issues arising from the decision included the technical challenges and costs for companies like Google, as well as free expression vs. an individual's right to privacy, and the impact on public figures (such as politicians) vs. ordinary citizens. Detractors suggested that the Court's decision would more likely "aid the powerful in attempts to rewrite history, than afford individuals more influence over their online identities" and noted that:

> Among the most troubling implications of the judgment are its impact on political speech and processes. Potential candidates for public office will now have a means of curating their own bespoke search results to ensure that only flattering information remains readily available to the public. The ruling is not limited to those embarrassing photos we wish we could banish from social media but includes news stories and other items of critical importance to an honest accounting of history.[3]

Another article, published in the *Ottawa Citizen* on May 18, 2014, was titled "Only a matter of time until 'right-to-be-forgotten' debate comes to Canada".

Throughout 2014-15, and continuing on into 2015-16, the ECJ decision and its possible implications was a popular subject at many access to information and privacy conferences, particularly those looking at the future of privacy. For the Alberta OIPC's Data Privacy event in January 2015, Jason Fung with Alberta Justice discussed jurisdictional issues associated with the decision.

[3] Stephens, Mark, "Only the powerful will benefit from the 'right to be forgotten'", *The Guardian*, May 18, 2014.


By the Numbers

100%
more complaint cases closed than in 2013-14

59
orders and decisions issued
(21% decrease from 2013-14)

120
media enquiries
(3% increase from 2013-14)

76
speeches and
presentations delivered
(4% increase from 2013-14)

341
Privacy Impact Assessments
submitted by HIA custodians
(8% decrease from 2013-14)

1311 number of cases closed
(excluding Intake cases)

FOIP **550** HIA **503** PIPA **258**

13% increase from 2013-14

1448 number of cases opened
(excluding Intake cases)

FOIP **589** HIA **528** PIPA **331**

1% increase in volume of cases since 2013-14
12% increase in volume of cases since 2011-12

37%
increase in self-reported breach
cases opened from 2013-14

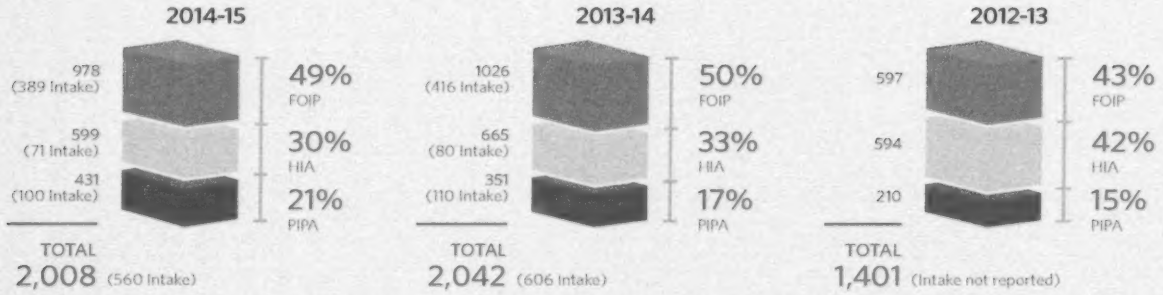
36%
increase in self-reported breach
cases closed from 2013-14

79%
decrease in requests to excuse
fees from 2013-14

108%
increase in files closed for requests
to excuse fees from 2013-14

Graph A: Total Cases Opened

Three Year Comparison



Graph B: Total Cases Closed

Three Year Comparison

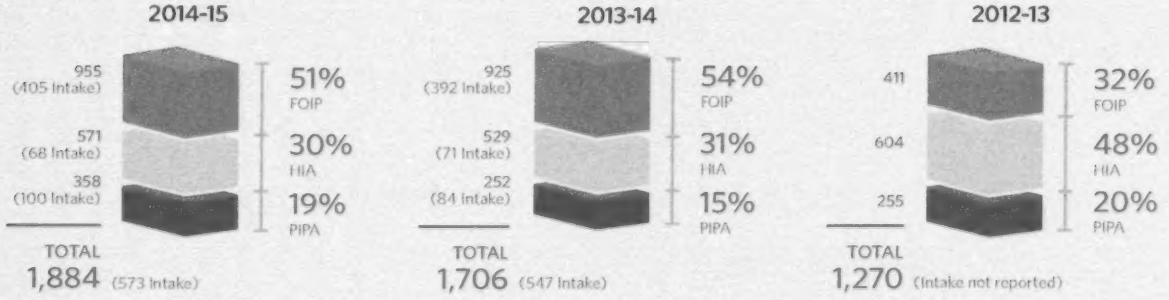


Table 1: Cases Opened by Case Type

FOIP	2014-15	2013-14	2012-13
Advice and Direction	0	1	4
Authorization to Disregard a Request	7	0	3
Complaint	85	91	125
Disclosure to Commissioner (Whistleblower)	1	1	-
Notification to OIPC	8	4	6
Engage in or Commission a Study	0	2	0
Excuse Fees	7	33	3
Investigation Generated by Commissioner	23	5	11
Offence Investigation	2	0	1
Privacy Impact Assessment	12	14	21
Request Authorization to Indirectly Collect	0	1	-
Request for Information	24	26	32
Request for Review	294	303	239
Request for Review 3rd Party	22	26	43
Request Time Extension	63	81	68
Self-reported Breach	41	22	41
Sub-Total	**589**	**610**	**597**
Intake Cases	**389**	**416**	**N/R**
Overall Total	**978**	**1026**	**597**

HIA	2014-15	2013-14	2012-13
Advice and Direction	0	0	0
Authorization to Disregard a Request	1	0	0
Complaint	39	50	27
Notification to OIPC	0	0	1
Engage in or Commission a Study	0	0	0
Excuse Fees	1	0	0
Investigation Generated by Commissioner	28	15	48
Offence Investigation	2	4	0
Privacy Impact Assessment	341	369	399
Request for Information	24	33	48
Request for Review	16	46	14
Request Time Extension	0	0	0
Self-reported Breach	76	68	57
Sub-Total	**528**	**585**	**594**
Intake Cases	**71**	**80**	**N/R**
Overall Total	**599**	**665**	**594**

PIPA	2014-15	2013-14	2012-13
Advice and Direction	0	0	1
Authorization to Disregard a Request	0	0	1
Complaint	121	75	52
Notification to OIPC	0	0	0
Engage in or Commission a Study	0	0	0
Excuse Fees	0	0	0
Investigation Generated by Commissioner	7	14	6
Offence Investigation	0	0	0
Privacy Impact Assessment	3	1	0
Request for Information	9	3	10
Request for Review	52	52	56
Request Time Extension	1	0	0
Request for Advance Ruling	0	0	0
Self-reported Breach	138	96	84
Sub-Total	**331**	**241**	**210**
Intake Cases	**100**	**110**	**N/R**
Overall Total	**431**	**351**	**210**

N/R - not reported

Notes: (1) See Appendix A for a complete listing of the cases opened in 2014-15.

(2) Only FOIP allows a 3rd Party to request a review of a decision to release 3rd party information to an applicant.

(3) Intake cases include determining whether parties coming to the OIPC are properly exercising the rights set out in FOIP, HIA and PIPA; whether the matters or issues identified by the parties are within the Commissioner's legislative jurisdiction; and investigating and trying to resolve certain requests or complaints.

Table 2: Cases Closed by Case Type

FOIP	2014-15	2013-14	2012-13
Advice and Direction	0	1	3
Authorization to Disregard a Request	4	1	3
Complaint	117	77	66
Disclosure to Commissioner (Whistleblower)	0	1	-
Notification to OIPC	8	4	6
Engage in or Commission a Study	0	0	0
Excuse Fees	25	12	3
Investigation Generated by Commissioner	7	6	2
Offence Investigation	0	0	1
Privacy Impact Assessment	16	13	15
Request Authorization to Indirectly Collect	0	1	-
Request for Information	29	22	33
Request for Review	230	258	163
Request for Review 3rd Party	24	26	21
Request Time Extension	64	90	58
Self-reported Breach	26	21	37
Sub-Total	**550**	**533**	**411**
Intake Cases	**405**	**392**	**N/R**
Overall Total	**955**	**925**	**411**

HIA	2014-15	2013-14	2012-13
Advice and Direction	0	0	0
Authorization to Disregard a Request	1	0	1
Complaint	42	15	23
Notification to OIPC	0	0	1
Engage in or Commission a Study	0	0	1
Excuse Fees	0	0	0
Investigation Generated by Commissioner	18	13	42
Offence Investigation	1	0	1
Privacy Impact Assessment	340	344	410
Request for Information	21	29	49
Request for Review	9	17	17
Request Time Extension	0	0	0
Self-reported Breach	71	40	59
Sub-Total	**503**	**458**	**604**
Intake Cases	**68**	**71**	**N/R**
Overall Total	**571**	**529**	**604**

PIPA	2014-15	2013-14	2012-13
Advice and Direction	0	0	1
Authorization to Disregard a Request	2	0	0
Complaint	114	50	113
Notification to OIPC	0	0	0
Engage in or Commission a Study	0	0	0
Excuse Fees	0	0	1
Investigation Generated by Commissioner	12	4	2
Offence Investigation	0	0	0
Privacy Impact Assessment	3	0	0
Request for Information	6	7	7
Request for Review	44	41	56
Request Time Extension	1	0	0
Request for Advance Ruling	0	0	0
Self-reported Breach	76	66	75
Sub-Total	**258**	**168**	**255**
Intake Cases	**100**	**84**	**N/R**
Overall Total	**358**	**252**	**255**

N/R - not reported

Notes: (1) See Appendix B for a complete listing of the cases closed in 2014-15.

(2) Only FOIP allows a 3rd party to request a review of a decision to release 3rd party information to an applicant.

(3) Intake cases include determining whether parties coming to the OIPC are properly exercising the rights set out in FOIP, HIA and PIPA; whether the matters or issues identified by the parties are within the Commissioner's legislative jurisdiction; and investigating and trying to resolve certain requests or complaints.

Table 3: Percentage of Cases Closed by Resolution Method

Under the Acts only certain case types can proceed to inquiry if the matters are not resolved at mediation/investigation. The statistics below are those case types that can proceed to inquiry (Request for Review, Request for Review 3rd Party, Request to Excuse Fees, and Complaint files).

RESOLUTION METHOD	NUMBER OF CASES (FOIP)	NUMBER OF CASES (HIA)	NUMBER OF CASES (PIPA)	TOTAL	%
Resolved by Mediation/Investigation	322	47	147	516	85%
Resolved by Order or Decision	54	2	8	64	10%
Resolved by Commissioner's Decision to Refuse to Conduct an Inquiry	2	1	1	4	1%
Withdrawn during inquiry process	14	1	1	16	3%
Discontinued during inquiry process	4	0	1	5	1%
Total	**396**	**51**	**158**	**605**	**100%**

FOIP Orders: 40 (53 cases); FOIP Decisions: 1 (1 case); HIA Orders: 2 (2 cases); PIPA Orders: 6 (8 cases)

Notes: (1) This table only includes Orders and Decisions issued that concluded/closed the file. See Appendix C for a list of all Orders, Decisions and Public Investigation Reports issued in 2014-15. A copy of all Orders, Decisions and Public Investigation Reports are available on the OIPC website www.oipc.ab.ca

(2) One FOIP case file was closed by Decision rather than by Order.

(3) One FOIP case file was closed by discontinuing the inquiry after a Decision had been issued.

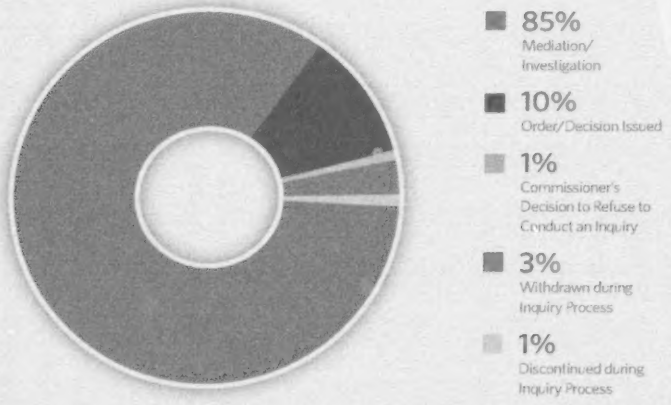
(4) Two PIPA case files that involved two different organizations were closed by a single Order.

(5) Some Orders, Decisions and/or Public Investigation Report Numbers were assigned to more than one case. Some cases had more than one Order and some had both an Order and a Decision.

(6) Orders and Decisions are recorded by the date the Order or Decision was signed, rather than the date the Order or Decision was publicly released.

(7) An inquiry can be discontinued due to a lack of contact with or participation of the applicant or complainant or the issues have become moot.

Graph C: Percentage of Cases Closed by Resolution Method



Of the 605 cases that could proceed to inquiry:

10% were resolved within 90 days

13% were resolved within 91 to 180 days

77% took more than 180 days to resolve*

**A number of complaint cases had been placed in abeyance in 2013-14 while the Office prioritized time-sensitive matters. Once the new office structure and staff were in place, dealing with the backlog became a priority. The 77% reflects the number of cases that had been in abeyance and were closed in the 2014-15 fiscal year.*

Table 4: Telephone Calls, Emails and Written Enquiries

FOIP	Number	Percentage
Public Bodies	207	26%
Individuals	581	74%
Total	**788**	**100%**

HIA	Number	Percentage
Custodians	476	54%
Individuals	409	46%
Total	**885**	**100%**

PIPA	Number	Percentage
Organizations	472	29%
Individuals	1,152	71%
Total	**1,624**	**100%**

Emails	**631**
Non-jurisdictional	**295**
Total	**4,223**

Regulation & Enforcement

Requests for Time Extensions under FOIP

Under section 11(1)(a) of the FOIP Act, a public body must make every reasonable effort to respond to a request no later than 30 calendar days after receiving the request, unless the time limit for response is extended under section 14.

Section 14(1) allows a public body to extend the time limit for responding by up to 30 days on its own authority in certain circumstances. An extension period longer than an additional 30 days requires the Commissioner's permission.

Section 11(2) states a failure by a public body to respond to a request within the 30-day time limit, or a time limit extended under section 14, is to be treated as a decision to refuse to access.

In seeking permission from the Commissioner to extend the response due date, a public body must establish that one of the conditions set out in section 14 has been met. Furthermore, since the FOIP Act is premised on timely processing of requests, an extension must be reasonable given the relevant circumstances.

In 2014-15, the OIPC received a total of 63 requests for permission to extend the response due date, a decrease of 22% from 2013-14. Of the requests received:

- 28 (or 44%) were granted as requested
- 22 (or 35%) were partially granted (extension period permitted less than the period requested by the public body)
- 12 (or 19%) were refused
- 1 (or 2%) was withdrawn by the public body

Of the 63 time extension requests received by the OIPC:

63% were made by provincial government ministries

16% were made by municipalities

13% were made by Boards

3% each were made by post-secondary institutions and a regional health authority

2% were made by Commissions

Privacy Impact Assessment Reviews

A privacy impact assessment (PIA) describes how new initiatives affect the privacy of individuals. Ideally conducted before implementation, a PIA is an exercise in due diligence and critical thinking that identifies privacy concerns so they can be addressed before implementation, heading off costly, post-production fixes and preventable privacy breaches. A good PIA includes a description of the initiative, explaining its benefits, an analysis of the legal authority to collect, use, or disclose health or personal information, an assessment of privacy risk and mitigation plans, and a description of the management and policy structure in place to ensure on-going privacy compliance.

PIA overview

In 2014-15, the OIPC accepted 326 PIAs. The largest portion (311 or 95%) of these PIAs was accepted under HIA because of that statute's mandatory PIA requirements. The OIPC accepted 13 PIAs from public bodies subject to the FOIP Act, while 2 PIAs were accepted from PIPA organizations.

As observed in the previous fiscal year, information sharing across organizations and jurisdictions continues to be a strong theme.

HIA

Similar to previous years, Alberta Health Services (AHS) and Alberta Health (AH) led the health sector, accounting for 33 and 15 accepted PIAs respectively. Alberta's other large health board, Covenant Health, provided 5 of this year's accepted PIAs. Both AHS and AH continue to maintain and update previously accepted PIAs for major systems, including patient registries, cancer screening programs, public health surveillance, organ and tissue donation, and general electronic medical records systems.

The OIPC accepted the first pharmacy PIA for real-time integration with Alberta Netcare, Alberta Health's provincial electronic records system. Real time integration allows pharmacies to use data feeds from Netcare health information repositories directly in their own systems, rather than looking up patient information in a separate web-browser interface, as has been the case for most Netcare users until now. Integration raises a number of interesting privacy issues in that the boundaries between previously separate systems become blurred. As such, custodians need to understand their own system, understand how the provincial system is interacting with theirs and understand their obligations under HIA for both systems. We expect more PIAs to be submitted for integration with Netcare in the coming years.

FOIP

The OIPC reviewed and accepted 13 PIAs from public bodies. Many of these PIAs covered topics related to education and youth, such as using Google apps for education at Mount Royal College, the new Teacher Workplace Information System from Alberta Education , and a new project at the Child Youth Data Lab from Alberta Human Services, describing a project to analyse the experiences of Alberta youth over time, using data sets from multiple stakeholders. Another PIA of interest was Service Alberta's PIA for Phase 1 of MyAlbertaDigitalIdentity. The initiative described by this PIA will eventually provide an identity management and online authentication service for citizens across Government of Alberta ministries and is intended to align with similar pan-Canadian identity management initiatives.

PIPA

This year, the OIPC accepted its first PIA for usage based auto insurance (UBI) from an organization preparing to enter the Alberta market. Under UBI programs, auto insurance customers can receive discounts based on their driving habits, which are recorded on a telematics device in the vehicle and transmitted to the insurance provider wirelessly. We expect to review further PIAs on this topic in the coming years.

Investigation Reports

Teacher names and email addresses used to send Minister's email

Alberta Education was found in contravention of the FOIP Act following an investigation into a mass email sent to teachers by the Minister of Education the previous year. The investigation revealed that the mailing list used by the Education Minister to contact teachers was created from the Alberta Teacher Registry and included both business and personal email addresses of 34,328 teachers.

The email addresses were collected by Alberta Education from teachers applying for certification, and from school authorities submitting information to update the Registry.

The investigation concluded that the FOIP Act authorized the use and disclosure of teacher names and business email addresses since this is information that is routinely disclosed in a business or professional context and no other personal information was revealed.

The use and disclosure of teacher names and personal email addresses, however, was not authorized under the FOIP Act.

Alberta Education agreed to implement the following recommendations:

- Remove personal email addresses from the Minister's mailing list.
- State, in all future mass email communications from the Minister to the teachers, the authority for the collection, use and disclosure of the teachers' personal information.
- Provide clear instructions to school authorities that only business email addresses assigned to teachers by their school authority or identified by teachers for business use be included in the submissions to Alberta Education.
- Update all notifications on any forms used to collect information for the Registry to include the purposes for which the information is collected.

Alberta Education, Investigation Report F2014-IR-02

Theft of unencrypted laptop containing health information

Medicentres Canada Inc. was found in contravention of HIA following an investigation into the theft of an unencrypted laptop containing health information from an information technology (IT) consultant working for Medicentres. The laptop contained billing information, including codes that revealed diagnosis and treatment information, for 621,884 Albertans.

The investigation found that Medicentres, acting as the physicians' information manager, contravened HIA by failing to take reasonable steps to safeguard health information on the laptop computer. Further, Medicentres did not provide guidance to the contracted IT consultant about the protection of health information.

Medicentres followed OIPC guidelines in responding to a privacy breach; however, it spent considerable time doing so. The investigation report recommended changes to Medicentres' breach response protocol to ensure that it includes timelines for notification.

The agreement between Medicentres and the physicians did not include any requirement that Medicentres report to the physicians about privacy concerns. As such, the physicians, who were ultimately responsible for HIA compliance, were not informed by Medicentres about the breach until nearly four months after it happened. The report recommended the implementation of an internal governance mechanism to ensure the physicians are aware of and engaged in decisions Medicentres makes on their behalf.

Medicentres Canada Inc., Investigation Report H2014-IR-01

Privacy Breach Reporting under HIA

In the wake of the Medicentres privacy breach (see Investigation Reports), the provincial government amended HIA to include mandatory reporting of privacy incidents to the individuals affected, the Commissioner and the Minister of Health. This amendment received Royal Assent on May 14, 2014, but has yet to be proclaimed in force. Therefore, privacy breach reporting remained voluntary under HIA throughout 2014-15. It is expected the the new reporting requirement will be proclaimed in force when regulations are written, sometime in the next fiscal year.

In 2014-15, custodians under HIA reported 76 incidents affecting the privacy of individuals, up from 68 in the previous fiscal year, a 12% increase. Common causes of incidents included misdirected communications, lost and stolen mobile devices that were unencrypted, and inappropriate use of health information by staff. The OIPC reviews every reported case of inappropriate use of health information to determine whether an offence investigation is warranted and sufficient evidence is available to prosecute.

Privacy Breach Reporting under FOIP

There is no requirement under the FOIP Act for public bodies to report privacy breaches to the Commissioner, or to the individuals affected. Despite this, public bodies reported 41 privacy breaches in 2014-15. This figure is almost double the 22 breaches reported last year (an 86% increase).

The most common causes of the breaches reported this year were misdirected communications, both via email and on paper, and the theft of unencrypted computers following break-ins to vehicles, offices and homes. It is particularly disturbing to see so many privacy breaches caused by the theft of unencrypted devices. The OIPC continually reminds all public bodies, custodians and organizations to follow this three-step guidance:

1. Do not store personal information on mobile devices. Rather, access your sensitive personal information remotely, over a secure channel.
2. If you must store personal information on a mobile device, store only what is necessary to limit your risk.
3. When storing limited personal information on a mobile device, make sure your device is properly encrypted – password protection alone is not enough.

Mandatory Breach Reporting under PIPA

Under PIPA, organizations must report to the Commissioner any loss, or unauthorized access or disclosure of personal information, where the organization determines a real risk of significant harm may result to the individuals concerned. Further, the Commissioner has the power to require organizations to notify affected individuals when a privacy breach presents a real risk of significant harm.

The following highlights significant privacy breaches and trends reported under PIPA in 2014-15 and the Commissioner's decisions regarding notification. Of the 76 PIPA self-reported breach files closed this year, the Commissioner issued decisions requiring that the organizations notify the affected individuals for 37 of these.

While the 76 closed self-reported breach files is somewhat higher than last fiscal year (66), the number of self-reported breaches received is up sharply this year from 96 to 138, representing a 44% increase over 2013-14.

Insider misuse of personal information

Many organizations have reasonable security arrangements in place to protect personal information against outside threats but remain vulnerable to misuse of personal information by employees. Employees inside two organizations used personal financial information to commit fraud and another exfiltrated personal information to a competing business.

An employee created fictitious insurance policies to improve their work record. The affected individuals experienced harm through these fraudulent transactions. The Commissioner also noted that the organization was not able to confirm whether the employee, who had been dismissed, had not copied the information elsewhere, contributing to her decision to require notification.

Human resources staff used employee financial information to commit fraud. Not all of the individuals whose information was exposed were victims of fraud before the rogue human resources staff members were arrested. Because there was clear evidence that some of the affected individuals had already been victims of fraud, there was a real risk of significant harm for the other individuals who hadn't experienced fraud. The Commissioner required the organization to notify the affected individuals.

In a third example of insider misuse, a collections agency employee copied client information and disclosed it to a former employee who was starting their own collections business. The competing collections agency began contacting the affected individuals implying that their accounts had been reassigned to the second agency. The Commissioner recognized the sensitivity of the debt-collection information, which could be used to cause financial loss, embarrassment and harassment by an unauthorized collection agency, and required the organization to notify all affected individuals.

The best defences against insider misuse are access controls that limit users' ability to access personal information to their business need to know, coupled with an audit program to ensure employees are following the organization's rules.

Allstate Insurance Company of Canada, P2014-ND-04
Home Depot of Canada Inc., P2014-ND-05
CBV Collection Services Ltd., P2015-ND-02

Malware and international e-commerce

Malicious software (malware) continues to be a significant cause of privacy breaches for online merchants. In both cases highlighted here, sensitive

credit card payment information was exposed to unknown parties via malware over extended periods (3 months and 14 months), increasing the risk the information was passed on. Both organizations recognized the risk and had already notified the affected individuals when they reported the breach to the OIPC. The organizations also reported the breaches to law enforcement and conducted internal investigations, leading to the replacement or patching of the affected systems. The Commissioner confirmed the organizations' assessment of the real risk of significant harm, noting the extended exposure as a factor in her decisions.

The two organizations mentioned below are registered and located in the United States. Despite this, the Commissioner routinely takes jurisdiction in situations like this because the personal information in question is collected from customers in Alberta via an e-commerce website. One side of the transaction is Alberta-based, creating a connection to Alberta for personal information involved in the privacy breach. In contrast, if all parts of a transaction take place outside Alberta and the responsible organization is registered and located outside Alberta, the Commissioner would be unlikely to take jurisdiction, despite the fact that Albertans may be affected, as there may not be sufficient connection to Alberta in that case.

Gingerbread Shed Corporation, P2014-ND-12
J.M. Smucker, P2014-ND-18

Social engineering

While technologically-oriented attacks such as hacking and malware continue to be a significant risk to the confidentiality of personal information, social engineering is also a threat. Social engineering refers to deceiving users or administrators into revealing confidential information.

An advisor at a financial services organization acted on fraudulent emails, believing they had been sent by customers. Instead, the emails had been sent by someone who had gained access to customer email accounts and who knew enough about the customers to deceive the advisor into believing the emails were genuine. When later confirming the transactions with the affected customers, the advisor discovered that the original email requests were fraudulent.

A credit application service used by car dealers was compromised by someone impersonating an employee, convincing a user with administrative privileges to reveal their authentication credentials. The attacker then accessed customer financial information and was even able to create an account to gain further access to personal information. Unfortunately, this is the second time this credit application service has been successfully attacked through social engineering – a similar incident was covered in last year's annual report.

In both of these cases, the Commissioner directed the organizations to notify the affected individuals because of the sensitivity of the personal information, and the fact that the information had been disclosed to unauthorized parties with malicious intent.

Transamerica Securities Inc., P2014-ND-01
DealerTrack Canada Inc., P2014-ND-09

Failure to wipe hard drive

Despite previous investigation reports and guidance from this Office, organizations still do not pay proper attention to securely deleting media before it is re-sold.

An organization sold a used computer to a customer who discovered personal information belonging to the previous owner on the hard drive. In following up on the incident, which was reported by the customer, the organization securely deleted the hard drive, but did not do an inventory of what information was stored on the computer, so could not properly assess the privacy risk to the original owner. Further, the computer in question may have been used as a floor model, so the organization could not say with certainty whether the information had been viewed by other customers. The inability to confirm what information was on the computer and the possibility that personal information could have been viewed while it was on the sales floor were factors that led the Commissioner to require the organization to notify the affected individual.

Best Buy Canada Ltd., P2014-ND-54

Offence Investigations

Under section 107 of HIA, it is an offence for any person to knowingly gain or attempt to gain access to health information, or collect, use or disclose health information in contravention of HIA. The Commissioner launched 2 investigations into possible offences under section 107 of HIA in 2014-15. One of these investigations has resulted in a successful prosecution. The other investigation is still underway.

HIA Conviction

On April 29, 2014, a medical laboratory assistant at the Calgary Laboratory Services (CLS) Patient Service Centre in Airdrie was found guilty of knowingly accessing the personal health information of 34 people in contravention of HIA and for falsifying documents under the *Criminal Code of Canada*.

The agreed statement of facts detailed that the assistant, who had already been terminated by CLS, had altered a lab test result and unlawfully accessed the health information of 34 people, including neighbours, acquaintances, and family members of a man she was in a personal relationship with. She pleaded guilty to one global charge for improper access of health information under HIA and three charges of uttering forged documents under the *Criminal Code*. She received a four month conditional sentence followed by eight months' probation in relation to the *Criminal Code* offences and a $500 fine in relation to the HIA offence.

While the $500 fine in this case is lower than what was levied under previous HIA offence convictions, the *Criminal Code* offences make the penalty for this matter very significant.

The Commissioner acknowledges CLS' cooperation and thorough internal investigation, which made use of detailed audit logs from its electronic lab record system, as important in obtaining this conviction.

Summary of Significant Decisions

Can an overly high fee estimate be a breach of the duty to assist?

An individual made a number of complaints, including that Alberta Health had overestimated the fee for his access request, and that this indicated an intention on the part of Alberta Health to dissuade him from his request. He also maintained that the person setting the fee was taking retaliatory action, as this person had been unsuccessful in defending Alberta Health's decision to withhold records in the inquiry relative to his earlier access request. The applicant argued that these things amounted to a breach by Alberta Health of its statutory duty to assist him.

The Adjudicator acknowledged it was not inconceivable that a public body employee might deliberately overestimate a fee to deter a request, or take punitive action, and that these things could amount to a breach of the duty to assist. However, she said that before such a finding could be made, the facts would have to be such that imputing an improper motive was the only reasonable conclusion. She found that the facts in the case did not support such a conclusion.

Alberta Health, Order F2014-20/H2014-01

Commissioner owes no deference to public body that has made a decision to withhold records

In the course of defending its decision to withhold information found in records responsive to an access request, Edmonton Police Service (EPS) relied on a 2008 decision of the Supreme Court of Canada, (*Dunsmuir v. New Brunswick*, (2008) 1 SCR 190), a case dealing with the deference courts owe to adjudicative bodies. EPS cited this case to support its argument that its decision to withhold records deserves deference, and should be reviewed on a standard of reasonableness.

The Adjudicator responded that the role of the Commissioner on an access request (and the Adjudicator's role as the Commissioner's delegate) is to reconsider the factors and reach a new and independent decision. The Adjudicator commented that while the Commissioner may wish to explain why she disagrees with the decision of a public body, she has the authority to make the determination as to whether access is to be granted, and in doing so, does not owe deference to the head of EPS who made the initial decision.

Edmonton Police Service, Order F2014-16

WCB authorized to collect personal information of others when performing covert surveillance of a claimant

An individual made a complaint that she had been surreptitiously videotaped by an investigator with the Workers' Compensation Board (WCB) without authority to do so. The individual had accompanied her mother to a store when she was videotaped. The individual's mother was a WCB claimant, and the WCB had undertaken surveillance of the mother in order to capture images of the mother for reasons related to the mother's claim.

The Adjudicator found that WCB had authority to collect the individual's personal information under section 33(b) of the FOIP Act (law enforcement). The Adjudicator held that this provision does not limit information that may be collected to information about the subject of a law enforcement investigation. She reviewed the surveillance tapes and noted that the individual's personal information was recorded only when she was close enough to her mother to be caught in the camera's field of vision. The WCB investigator was attempting to capture images of the mother in a variety of situations, performing a variety of tasks, and it would likely be difficult for the WCB to covertly record a WCB claimant in public places, in a variety of situations, without also recording images of other individuals. On this basis the Adjudicator concluded the WCB investigator had complied with the FOIP Act.

Workers' Compensation Board, Order F2014-37

FOIP Act discretionary disclosure exceptions do not apply to list of high-risk employers

The applicant asked Alberta Jobs, Skills, Training and Labour (JSTL) for information relating to the province's "highest-risk employers" relative to compliance with occupational health and safety standards. JSTL withheld the information, relying, in part, on the FOIP Act's discretionary exceptions to disclosure (law enforcement - section 20(1), advice to government - section 24(1), and information readily available to the public - section 29(1)), as well as on the Act's mandatory exception for information harmful to business interests under section 16. The applicant requested a review of that decision.

The Adjudicator decided to deal with the discretionary exceptions to disclosure first, and to review application of the mandatory exception only if none of the discretionary ones were held to apply. As to the discretionary exceptions, he found that disclosure of the employers on the list could not reasonably be expected to harm a law enforcement matter, or to harm the effectiveness of investigative techniques and procedures used in law enforcement. The Adjudicator also found that disclosure could not reasonably be expected to reveal advice, nor was it information that was readily available to the public.

Accordingly, the Adjudicator concluded that a review of the application of section 16(1) of the FOIP Act (harm to business interests) could proceed. [In the result, JSTL decided not to rely on the section 16 exception, and disclosed the records that had been at issue in the inquiry.]

Alberta Jobs, Skills, Training and Labour, Decision F2014-D-01

Judicial Reviews and Other Court Decisions

Imperial Oil Limited v. Alberta (Information and Privacy Commissioner)

2014 ABCA 231, which upheld *Imperial Oil Limited v. Calgary (City)*, 2013 ABQB 393, which quashed Order F2005-030. Leave to appeal to the Supreme Court of Canada dismissed 2015 SCC No. 36098, February 19, 2015

The City of Calgary (the City), itself a public body under the *Freedom of Information and Protection of Privacy Act* (the FOIP Act), made an access request to Alberta Environment, another public body, for an agreement (the Agreement) reached by Imperial Oil Limited (Imperial) and Alberta Environment (through the Environment Minister) following mediation in the context of regulatory proceedings under the *Environmental Protection and Enhancement Act* (EPEA). Alberta Environment, who was a party to the Agreement, refused to disclose the Agreement to the City. As an "Affected Party" (as defined in the FOIP Act), Imperial objected to disclosing the Agreement to the City.

The Agreement addressed the remediation of land in Calgary, which was contaminated when Imperial, who was a previous owner of the land, had released hydrocarbons and lead on it. Imperial subsequently sold the land to its subsidiary, which developed the land as a residential area. The need to remediate the land, to what standard, and the parties' responsibilities were the subject of protracted regulatory and court proceedings. Alberta Environment issued environmental protection orders, which Imperial contested in regulatory proceedings. Ultimately, after Imperial appealed the environmental protection orders to the Environmental Appeals Board (the Board), but before the appeals were heard, Alberta Environment and Imperial engaged in mediation and resolved the matters between them. The Agreement comprised that resolution. Alberta Environment then cancelled the environmental protection orders.

Alberta Environment released parts of the Agreement to the public and, given that the Agreement impacted the City, released additional parts and details to the City. Alberta Environment refused the City's request for further disclosure. The City asked the then-Information and Privacy Commissioner (the Commissioner) to review Alberta Environment's refusal to disclose the Agreement. The Commissioner convened an inquiry to hear and determine the matter.

The Commissioner considered whether the Agreement was exempt from disclosure under section 16 of the FOIP Act, which is the "harm to business interests" exception to disclosure. The Commissioner found that most of the information in the Agreement was not Imperial's commercial, financial, labour relations, scientific or technical information (section 16(1)(a)), or was not information that was supplied by Imperial to Alberta Environment in confidence (section 16(1)(b)). The Commissioner observed that the Agreement was ambiguous as to whether it was to be kept confidential, as some clauses spoke of confidentiality while others spoke of disclosure. He held that it could not be concluded that the Agreement was to be kept confidential. As neither section 16(1)(a) or section 16(1)(b) was met, the Commissioner concluded that it was unnecessary for him to decide whether section 16(1)(c) was met.

Section 24(1) of the FOIP Act exempts from disclosure advice developed by or for public bodies. The Commissioner found that section 24(1) did not apply to exempt the Agreement from disclosure because that provision protects information generated during the decision-making process, but not the decision itself (in this case the Agreement), from public access. As Alberta Environment and Imperial were involved in developing the Agreement, it was not prepared by or on behalf of a public body as section 24(1)(a) requires.

The Commissioner found that disclosure of the Agreement would not cause the postulated economic harm to the Board and therefore section 25 of the FOIP Act did not apply to bar disclosure. Withholding the Agreement was not necessary to enable Alberta Environment to fulfill its mandate of ensuring that responsible parties met their remediation obligations under the EPEA.

The Commissioner held that the Agreement was not subject to privilege such that section 27 of the FOIP Act barred its disclosure. The communications giving rise to the Agreement could be privileged, but not the Agreement. The Wigmore criteria did not apply to cloak the Agreement in privilege. The public interests engaged by the dispute between Alberta Environment and Imperial, and the transparency associated with, and required by, that process meant the Agreement itself could not be privileged.

The Commissioner issued Order F2005-030, which ordered Alberta Environment to disclose the Agreement to the City. Imperial applied to the Court of Queen's Bench for judicial review of Order F2005-030.

The Court held that the Commissioner gave inadequate reasons in support of his conclusion that the Agreement did not contain commercial information, and that the scientific and technical information in the Agreement was that of a third party.

The Court found that "The fact that the Agreement was negotiated should not be a reason to exempt it from section 16(1)(b)." The Court held that the Commissioner's finding that the Agreement was not confidential incorrectly interpreted the EPEA to remove the Board's ability to mediate a resolution between parties.

The Court also found that the Commissioner incorrectly modified the legal test for privilege to add public policy requirements. The test for privilege was satisfied and the Commissioner's decision was incorrect. The Court held that confidentiality was important and could not be undermined. The Court quashed Order F2005-030.

The Commissioner appealed the decision of the Court of Queen's Bench.

The Court of Appeal struck the appeal on the ground that the Commissioner had no standing to appeal. The Court of Appeal distinguished between standing to appeal and the ability to make submissions on appeals launched by third parties.

The Court of Appeal held that prior appeals by the Commissioner and other tribunals carried no weight, and the City's unwillingness to appeal did not establish a right of appeal in the Commissioner.

Despite striking the appeal on the ground that the Commissioner had no standing to appeal, the Court of Appeal nevertheless decided the issues in *obiter dicta*, noting that it was "warranted given their importance". The Court of Appeal held that the Agreement was exempt from disclosure under both section 16 and section 27 of the FOIP Act, and upheld the decision of the Court of Queen's Bench.

The Commissioner applied to the Supreme Court of Canada for leave to appeal. On February 19, 2015, the Supreme Court of Canada dismissed the Commissioner's application.

Medicentres Canada Inc. v. Alberta (Information and Privacy Commissioner)

2014 ABQB 489

A laptop computer owned by an information technology consultant who was performing services for Medicentres Canada Inc. (Medicentres) was stolen. The laptop contained the health information of 621,884 Albertans who were patients of Medicentres.

The Commissioner commenced an investigation of Medicentres under section 84(1)(a) of the *Health Information Act* (HIA). Medicentres brought an application for judicial review, seeking a prohibition order to prohibit the Commissioner from concluding the investigation and, on the ground of procedural unfairness, to prohibit the Commissioner from publishing any report of the investigation that included any references to certain emails; any comment or statement that Medicentres had authority from physicians to provide information in response to the investigation; and any comment, finding or recommendations about the loss of the laptop.

Medicentres also asked for an interim order staying the investigation until the judicial review could be heard, and a publication ban on the investigation report pending the application for prohibition.

The Court said that the application before it was essentially an injunction application, and that the tests for a stay are the same as those for an injunction: serious question to be tried, irreparable harm and balance of convenience.

The Court held that a breach of procedural fairness was a serious issue to be tried. However, as to irreparable harm, there would be no direct consequences against Medicentres or the physicians flowing from the final report. Their legal rights as among themselves would be unaffected. No order would be made against them. Therefore, the Court held that Medicentres did not meet the burden of establishing that it would suffer irreparable harm if the investigation report was finalized without any further consultation, input or review by Medicentres.

As to balance of convenience, the Court said it must weigh the interests of Medicentres against the interests of the public in having the investigation concluded and a public report issued. The Court held that there was a public interest in having recommendations made as soon as possible, so that any glitches in the system could be addressed.

Finally, the Court held that a publication ban was not appropriate, as this was clearly a matter involving the public interest, there were no elements of confidentiality to the investigation, and the media was not notified.

The Court dismissed Medicentres' application for a stay or for an interim injunction against issuance of the final report in the investigation. On October 10, 2014, Medicentres filed a discontinuance of the judicial review.

Covenant Health v. Alberta (Information and Privacy Commissioner)

2014 ABQB 562 - Judicial review of Order F2013-24/H2013-02

The applicant applied to Covenant Health (Covenant) for access to her personal information so that she could learn the reasons for being banned from its premises and having restrictions imposed on her visiting privileges with her parents.

Covenant withheld information on the basis that it was health information under the *Health Information Act* (HIA) or that it was personal information and disclosure would be an unreasonable invasion of personal privacy under section 17 of the FOIP Act. Covenant also withheld information as being "advice from officials" under section 24 the FOIP Act.

At inquiry, the Adjudicator found that the information was not health information under HIA, but that the FOIP Act applied. The Adjudicator found that disclosure of some information would not be an unreasonable invasion of the personal privacy of the agent of the applicant's parents because that individual was acting as an agent in a representative capacity and the personal information was necessary for a fair determination of the applicant's rights. The Adjudicator also ordered Covenant to reconsider its decision about withholding information that was advice from officials. Finally, the Adjudicator ordered Covenant to conduct a new search for records as it had not met its duty under section 10(1) of the FOIP Act.

On judicial review, the Court held that section 11(2) of HIA prohibited Covenant from disclosing the health information of the applicant's parents; that disclosure of the personal information of the agent of the applicant's parents would contravene section 17(1) of the FOIP Act; that Covenant's decision to withhold information under section 24 of the FOIP Act was reasonable; and that Covenant had met its duty under section 10(1) of the FOIP Act. The Court quashed Order F2013-24/H2013-02.

Imperial Oil Limited v. Alberta (Information and Privacy Commissioner)

2014 ABCA 276

Pursuant to a consent order, the Court of Queen's Bench sealed the Remediation Agreement and the confidential addendum to the Commissioner's reasons in Order F2005-030 (the Sealed Records). The consent order provided that the Court was to return the Sealed Records to the Commissioner at the conclusion of the Court proceedings.

The Court of Appeal in 2014 ABCA 231 determined that it would keep one archival copy of the Sealed Records, as was its practice. The Court of Appeal invited the parties to address the Court if that arrangement was not satisfactory.

The Commissioner provided a submission on why the Sealed Records should be returned to the Commissioner, arguing that section 56(5) of the FOIP Act was mandatory in that it required the Commissioner to return records that the Commissioner required to be produced under section 56. The Court of Appeal disagreed with the Commissioner's interpretation of section 56 and stated that it would instruct the Registrar to maintain the Sealed Records in the Court's file, in accordance with the usual practice.

Alberta Treasury Branches v. Alberta Union of Provincial Employees

2014 ABQB 737 - Judicial Review of Order F2012-09 and Decision F2013-D-01

The applicant applied to Alberta Treasury Branches (ATB) for records containing information about the number of employees and classifications excluded from the bargaining unit, and other classification and job descriptions of excluded positions.

ATB declined to respond to the access request on the basis that the FOIP Act did not apply to the records, since section 4(1)(r) of the FOIP Act says that records in the custody or under the control of a treasury branch are excluded from the FOIP Act.

At inquiry, the Adjudicator found that there is a distinction between ATB as a corporate entity, and a treasury branch, which is an entity created by ATB. She determined that, under the FOIP Act, there are two categories of records in the custody or control of ATB that are subject to the FOIP Act: records in the custody or control of ATB, but not a treasury branch, and records that document specified kinds of non-arm's length transactions. Since the Adjudicator found that ATB had not addressed the question of whether there were responsive records in the custody or control of ATB, but not a treasury branch, and that ATB had not conducted a search for any such records, she ordered ATB to do so.

ATB applied for judicial review of Order F2012-09. During the judicial review, the Court determined that the issue of whether section 36(3) of the *Alberta Treasury Branches Act* (ATBA) affected the interpretation of section 4(1)(r) of the FOIP Act had not been addressed in Order F2012-09. The Court declined to decide that issue in the first instance, and remitted it to the Adjudicator.

The Adjudicator issued Decision F2013-D-01, in which she determined that section 36(3) of the ATBA is a transitional provision, the general purpose of which is to provide how a new Act applies to situations that arose before the coming into force of the Act and that are affected by its passage. The Adjudicator found that section 36 was intended to establish how the ATBA applied to situations that arose before the coming into force of the ATBA. The Adjudicator further found that section 36(3) does not apply to section 4(1)(r) of the FOIP Act, as section 4(1)(r) does not refer to a treasury branch as a branch of the Treasury Department created under the former *Treasury Branches Act*, but to a treasury branch created under the ATBA.

ATB applied for judicial review of Decision F2013-D-01.

The Court consolidated the judicial review applications for both Order F2012-09 and Decision F2013-D-01. The Court held that the standard of review to be applied to the Adjudicator's findings and statutory interpretations was reasonableness. Since the Adjudicator's reasons were justifiable, transparent and intelligible, there was no basis for interfering with the Adjudicator's reasonable conclusion. The Court dismissed the judicial reviews of Order F2012-09 and Decision F2013-D-01.

Alberta Teachers' Association v. Information and Privacy Commissioner

2014 ABCA 432, which reversed in part 2013 ABQB 283

In 2013 ABQB 283, the Court of Queen's Bench ordered the disclosure of certain records on judicial review. The Commissioner appealed the Court's disclosure order.

The Court of Appeal struck the appeal on the ground of mootness and on the ground that the Commissioner had no standing to appeal.

However, since the Alberta Teachers' Association had argued mootness and since it had no further interest in the information to which it had requested access, the Court of Appeal decided to stay the disclosure direction of the Court of Queen's Bench.

Calgary (Police Service) v. Alberta (Information and Privacy Commissioner)

2014 ABQB 791 – Judicial Review of Order F2013-12

An individual (the Complainant) complained to the Commissioner that that the Calgary Police Service (CPS) disclosed the Complainant's personal information contrary to the FOIP Act when a police officer provided a collision report in its entirety to a driver with whom the Complainant has been involved in a collision. The collision report provided to the driver contained the Complainant's name, address, home and work telephone numbers, driver's licence number and date of birth.

At inquiry, the Adjudicator found that the disclosure of some of the personal information was authorized by the *Traffic Safety Act* (TSA). However, the Adjudicator found that, by providing the entire collision report, the police officer had disclosed more personal information tha., was necessary to ensure that the Complainant and the other driver met their legal obligations to each other arising from the collision. The Adjudicator noted that the TSA does not require a police officer to provide an entire collision report to an individual involved in an accident, and that this legislation does not require the exchange of birthdates or phone numbers.

The Adjudicator ordered the CPS to cease disclosing more of the Complainant's personal information than was necessary from the collision report.

The CPS applied for judicial review of Order F2013-12.

The Court held that interpretation of the TSA was intimately related to the Commissioner's core functions under the FOIP Act relating to the disclosure of personal information, and involved interpreting sections of the TSA closely connected to the Commissioner's functions. Therefore the reasonableness standard applied to the Adjudicator's decision concerning both the FOIP Act and the TSA. The Adjudicator's decision provided a reasonable justification for her order, and the reasoning was transparent and intelligible. The Court dismissed the judicial review application.

The Alberta Teachers' Association v. Information and Privacy Commissioner

Oral decision of Ouellette J., Action No. 0803-05729, January 9, 2015 - Judicial Review of Order P2007-014.

The Alberta Teachers' Association (ATA) published the names of the Complainants and the Complainants' places of work in the ATA News, in conjunction with a statement that the Complainants were no longer required to adhere to the ATA's Code of Professional Conduct. The Complainants complained to the Commissioner that the ATA published their personal information, contrary to the *Personal Information Protection Act* (PIPA).

At inquiry, the Adjudicator held that the information in the ATA News article was the Complainants' personal information and the disclosure was not excluded from PIPA by virtue of section 4(3)(c) (journalistic purposes). The Adjudicator also held that the ATA disclosed the Complainants' personal information contrary to section 7 (consent or other authorization to disclose without consent) and section 19 (disclosure for purposes that are reasonable) of PIPA.

The Court of Queen's Bench quashed Order P2007-014 on the ground that the Commissioner lost jurisdiction when he did not complete an inquiry within 90 days of receiving a request for review as required by section 50(5) of PIPA, and did not extend the time within the 90 days. A majority of the Court of Appeal upheld the decision of the Court of Queen's Bench.

The Supreme Court of Canada decided that the Commissioner did not lose jurisdiction. The Supreme Court reinstated Order P2007-014 and, on the recommendation of the Commissioner, remitted the matter to the Court of Queen's Bench to consider the issues not previously dealt with and resolved on the judicial review.

The Court of Queen's Bench held that the Adjudicator's decisions under section 4(3)(c) and section 19 of PIPA were unreasonable, and quashed Order P2007-014. The Court chose not to go on to decide the alternative issues of section 7 and section 8 of PIPA.

The Court also said that, had the Court been required to make a ruling under section 2(b) of the *Canadian Charter of Rights and Freedoms*, the Court would have found that PIPA breached section 2(b) and was not saved by section 1, since the Court was bound by the ruling of the Supreme Court of Canada in *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*, 2013 SCC 62. Finally, the Court saw no need to deal with whether there were violations of the *Alberta Bill of Rights*.

Education & Outreach

The mandate of the OIPC includes a strong commitment to education and outreach. From publications to presentations and consultations, the Office continues to raise public awareness of the access to information and privacy rights under the FOIP Act, HIA and PIPA; provide guidance and direction to stakeholders to enhance compliance; and facilitate opportunities for the public and stakeholders to comment on the administration of the Acts, OIPC processes, and access and privacy issues in general.

The following are highlights of the informational and educational activities undertaken by the OIPC in 2014-15.

Presentations, Forums and Workshops

In 2014-15, the Commissioner and OIPC staff participated in 76 presentations, training sessions or speaking engagements, provincially and nationally. These events focused on building awareness about issues in access and privacy, and the application of the FOIP Act, HIA and PIPA.

The OIPC continued its involvement in the Legislative Assembly of Alberta's School at the Legislature program, which provides the Office with an opportunity to teach young Albertans about access and privacy.

Committee support was again provided by the Office for the University of Alberta's annual Access and Privacy Conference, and the Commissioner and OIPC senior leadership were involved in a panel discussion at the event.

The following highlight some of the presentations, forums and workshops from 2014-15.

Data Privacy Day

Data Privacy Day is internationally recognized on January 28 and is centred on respecting privacy, safeguarding data and enabling trust. To celebrate the day, the OIPC hosted a forum in Calgary, which included presentations on cloud computing, the relationship between gender, privacy and equality in online social networking, and accountability and consent for privacy practices.

Right to Know Week Forums

Established in 2002 by access to information advocates, Right to Know is a globally celebrated annual event that promotes access to information as a cornerstone of democracy and good governance. In honour of access to information in Alberta, the OIPC hosted forums in Calgary and Edmonton. Among the topics discussed were the use and benefits of open data in municipalities, complexity in access requests, how information management practices support the right to access, and a presentation by Robert C. Clark Award recipient Karen Kleiss.

Around the World Panel Discussion

In May 2014, the Kule Institute for Advanced Study at the University of Alberta held its second Around the World conference, this time focusing on Privacy and Surveillance in the Digital Age. The Commissioner participated as part of a panel discussing citizens' attitudes towards privacy and surveillance, the impact of social media, Big Data, and the adequacy of existing legal structures. The Around the World Conference website describes these events as "an experiment that brings together a research dialogue without the environmental cost of traditional conferences. Institutes and researchers are invited to participate either through presenting or by joining in the discussion. The conference is live-streamed." The 2014 event included participants from across Alberta, as well as the U.S., Netherlands, Australia, Ireland and more.

Federation of Medical Regulatory Authorities

The Commissioner and Director, Compliance and Special Investigations were pleased to attend the Annual General Meeting and Conference of the Federation of Medical Regulatory Authorities of Canada, held in Saskatoon in June 2014, to present a session focusing on privacy issues in an eHealth environment. Topics covered included governance and accountability, as well as the physician's role in protecting the confidentiality of patient information.

Regulator Expectations and Responses to Breaches Panel Discussion

In March 2014, the Commissioner participated in a one-day event titled "Data Breaches: Avoidance, Preparedness and Response" hosted by Osgoode Hall Professional Development. The Commissioner participated on a panel that discussed Regulator Expectations and Responses to Breaches. Topics covered included notable trends in breach incidents and reporting, resources made available by regulators to assist organizations in preventing and responding to breaches, and proposed amendments to Alberta's HIA to address mandatory breach reporting and notification.

Privacy Breaches Webinar

In May 2014, the OIPC conducted a privacy breaches webinar for the Conference Board of Canada where the Office shared the lessons learned from mandatory breach reporting under PIPA. The topics covered included how to prepare for a breach, what to do when it happens, avoiding breaches and reporting to the Commissioner. At the end of the session, participants were invited to play an interactive session of "Let's play... RROSH or No RROSH." Fact scenarios were sourced from actual breach reports and participants were asked to determine if the incident may or may not result in real risk of significant harm, which would trigger the reporting requirement under section 34.1 of PIPA.

PIA Training

The OIPC continued to offer quarterly Privacy Impact Assessment (PIA) training in 2014-2015 with special sessions for health sector participants. This initiative began last year to make up for the Government of Alberta's cessation of physician office system privacy support, as mentioned in the 2013-14 Annual Report. Aside from a large volume of learners from the health sector, many participants came from the private and public sectors as well.

Collaboration with Other Jurisdictions

The OIPC continued its collaboration with Canadian and international information and privacy authorities on topics of mutual interest. This collaboration includes comments on federal legislation, developing guidance on tools that have implications on access and privacy, and joint resolutions with federal, provincial and territorial Information and Privacy Commissioners and Ombudspersons.

Commissioners Comment on Federal Legislation

Both the federal Bill C-13, *Protecting Canadians from Online Crime Act*, and Bill C-51, *Anti-terrorism Act, 2015*, drew concern from the information and privacy regulators across Canada. In joint letters to the standing committees responsible for reviewing the legislative amendments, a range of issues were identified regarding the implications for access and privacy rights.

Guidance for Online Consent in the Private Sector

Alberta's Commissioner, along with the Privacy Commissioner of Canada and Information and Privacy Commissioner of British Columbia, outlined some of the key considerations for obtaining meaningful online consent. Under private sector privacy legislation, organizations are required to obtain meaningful consent before collecting, using and disclosing personal information. The guidance was released in May 2014.

Guidance on Body-Worn Cameras

Numerous law enforcement agencies across Canada, including Calgary Police Service and Edmonton Police Service, are using, or proposing to use, body-worn cameras. Federal, provincial and territorial Information and Privacy Commissioners and Ombudspersons urged law

enforcement agencies to carefully consider significant access and privacy risks before equipping officers with body-worn cameras. The guidance, which was released in February 2015, highlighted a number of issues and provided recommendations to help ensure access and privacy rights are upheld.

Global Privacy Sweep

For the first time, the OIPC participated in the Global Privacy Enforcement Network's annual Privacy Sweep. In 2014, the focus of the online Privacy Sweep was on mobile apps. In total, 21 Alberta-based mobile apps in the private, public and health sectors were analyzed. More than 1,200 mobile apps were looked at worldwide by 26 privacy enforcement authorities.

Following the Privacy Sweep, the Commissioner along with 23 privacy enforcement authorities from around the world called on app marketplaces to make it mandatory for mobile app developers to post links to privacy policies prior to download if the apps collect personal information.

Statement on National Security and Law Enforcement Measures

In a joint statement released in October 2014, Information and Privacy Commissioners and Ombudspersons across Canada called on the federal government to adopt an evidence-based approach for any new legislative proposal granting additional powers for intelligence and law enforcement agencies; to engage with Canadians in an open and transparent dialogue on whether new measures are required; and to ensure effective oversight is included in any legislation establishing additional powers for intelligence and law enforcement agencies.

Joint Resolution on Canadians' Access and Privacy Rights in the Era of Digital Government

In November 2014, Canada's access to information and privacy guardians recognized that the digital era has brought both tremendous opportunities and new challenges for access and privacy rights. As part of a joint resolution, federal, provincial and territorial governments were called on to review and modernize their information management practices.

Independent Research

To draw attention to a key issue that the Commissioner has commented on publicly, the OIPC commissioned independent research on government information sharing.

Government Information Sharing: Is Data Going Out of the Silos, Into the Mines?

This paper analyzes various Canadian and international government sharing initiatives with a perspective on privacy. It provides a framework for analysis of these projects, identifies project risks and strategies to mitigate risks, and broadly examines actions taken to protect privacy in the context of multi-stakeholder citizen-centred information sharing projects.

Media Requests

The OIPC received 120 media enquiries during the year. The issues receiving the most attention included:

- The use of body-worn cameras and facial recognition software by the Calgary Police Service, and the subsequent investigation announcement by the Commissioner.
- Announcement of the investigation into potential interference in responding to the Government of Alberta's FOIP requests.
- Status of PIPA following the Supreme Court of Canada ruling that PIPA was unconstitutional and the subsequent amendments to ensure its validity.
- Amendments to the *Health Information Act*, including a provision for mandatory breach notification.

Robert C. Clark Award

Named after Alberta's first Information and Privacy Commissioner, the Robert C. Clark Award recognizes an individual, group or organization that has contributed significantly to advancing access to information in Alberta.

In 2014, Karen Kleiss received the award for her efforts to obtain information from the Alberta government concerning the number of children who died in provincial care. As a reporter for the *Edmonton Journal*, Ms. Kleiss authored the "Fatal Care" series of articles in November 2013, which resulted in the reform of government legislation and policy.

An independent, three-person panel made up of subject matter experts with extensive experience in the field reviewed the nominations and selected the award recipient. In selecting Ms. Kleiss, the panel cited her efforts as a "public demonstration of how the [access to information] law works, including the process of review by the Information and Privacy Commissioner."

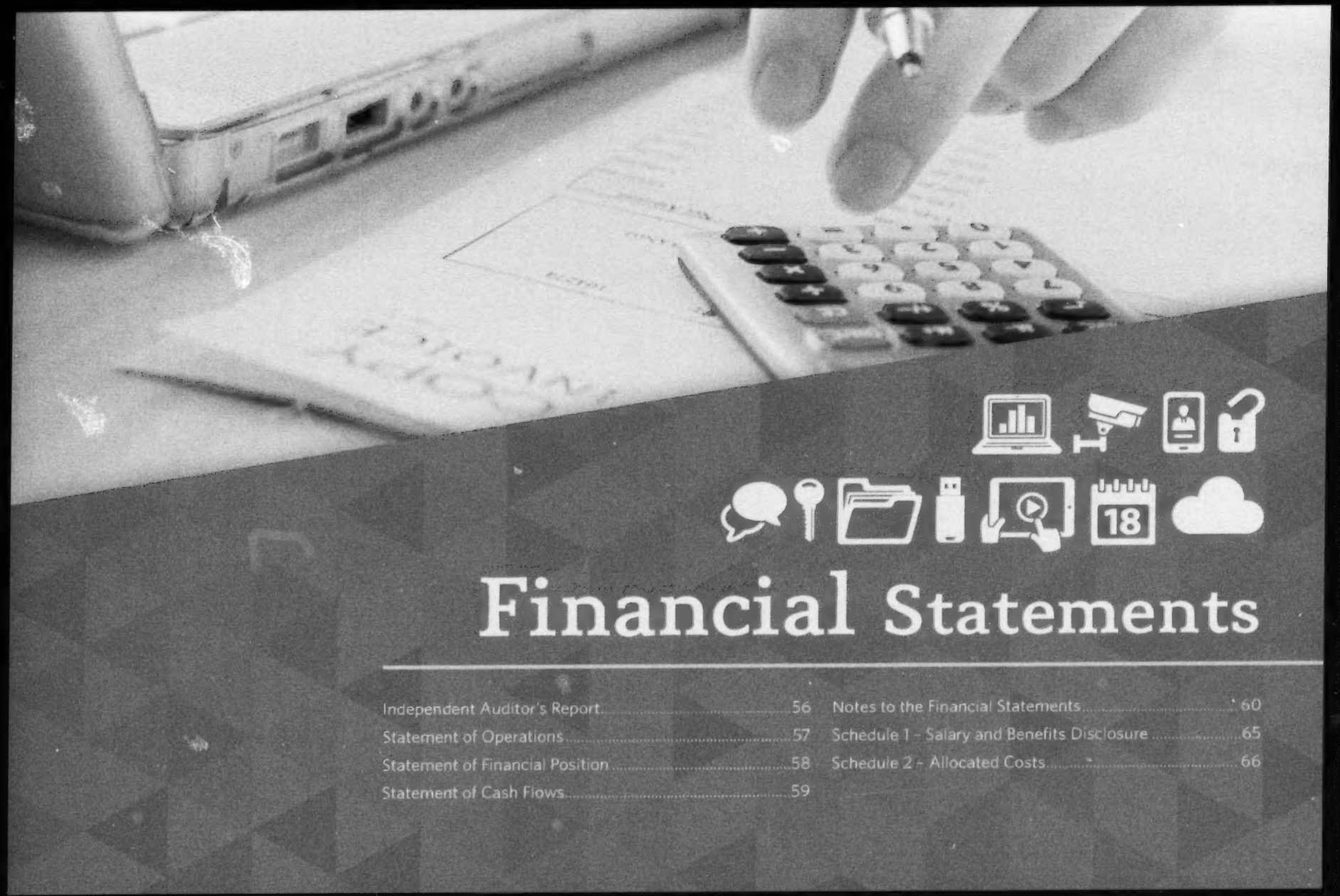
The selection panel members were:

- Kevin Dunion, Executive Director, Centre for Freedom of Information, University of Dundee, and former Scottish Information Commissioner
- Gary Dickson, former Saskatchewan Information and Privacy Commissioner
- Maria MacDonald, Information and Privacy Commissioner, Prince Edward Island

@ABoipc

#finally

The OIPC officially joined Twitter in June 2014. The social media platform is another method the Office uses to engage with Albertans and stakeholders and share the latest news and information about access and privacy issues at home and around the world.



Financial Statements

Independent Auditor's Report 56
Statement of Operations 57
Statement of Financial Position 58
Statement of Cash Flows 59
Notes to the Financial Statements 60
Schedule 1 - Salary and Benefits Disclosure 65
Schedule 2 - Allocated Costs 66

AUDITOR GENERAL *Alberta*

Independent Auditor's Report

To the Members of the Legislative Assembly:

Report on the Financial Statements

I have audited the accompanying financial statements of the Information and Privacy Commissioner, which comprise the statement of financial position as at March 31, 2015, and the statements of operations and cash flows for the year then ended, and a summary of significant accounting policies and other explanatory information.

Management's Responsibility for the Financial Statements

Management is responsible for the preparation and fair presentation of these financial statements in accordance with Canadian public sector accounting standards, and for such internal control as management determines is necessary to enable the preparation of financial statements that are free from material misstatement, whether due to fraud or error.

Auditor's Responsibility

My responsibility is to express an opinion on these financial statements based on my audit. I conducted my audit in accordance with Canadian generally accepted auditing standards. Those standards require that I comply with ethical requirements and plan and perform the audit to obtain reasonable assurance about whether the financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditor's judgment, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the entity's preparation and fair presentation of the financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of accounting estimates made by management, as well as evaluating the overall presentation of the financial statements.

I believe that the audit evidence I have obtained is sufficient and appropriate to provide a basis for my audit opinion.

Opinion

In my opinion, the financial statements present fairly, in all material respects, the financial position of the Office of the Information and Privacy Commissioner as at March 31, 2015, and the results of its operations, its remeasurement gains and losses, and its cash flows for the year then ended in accordance with Canadian public sector accounting standards.

Original signed by
Merwan N. Saher, FCA

Auditor General
June 16, 2015
Edmonton, Alberta

Office of the Information and Privacy Commissioner

Statement of Operations

Year ended March 31, 2015

	2015 Budget	2015 Actual	2014 Actual
Revenues			
Prior Year Expenditure Refund	$ -	$ 3,024	$ 4,775
Other Revenue	-	291	567
	-	3,315	5,342
Expenses - Directly Incurred (Note 3b)			
Salaries, Wages, and Employee Benefits	$ 5,757,500	$ 5,183,369	$ 4,781,805
Supplies and Services	1,225,500	1,587,093	1,293,633
Amortization of Tangible Capital Assets	74,000	83,876	56,556
Total Expenses	7,057,000	6,854,338	6,131,994
Net Operating Results	$ (7,057,000)	$ (6,851,023)	$ (6,126,652)

The accompanying notes and schedules are part of these financial statements.

Financial Statements

Office of the Information and Privacy Commissioner

Statement of Financial Position

As at March 31, 2015

	2015	2014
Assets		
Cash	$ 100	$ 100
Accounts Receivable	3,271	34
Prepaid Expenses	295	905
Tangible Capital Assets (Note 4)	202,520	267,745
	$ 206,186	$ 268,784
Liabilities		
Accounts Payable and Accrued Liabilities	$ 408,482	$ 461,701
Accrued Vacation Pay	537,555	479,201
	946,037	940,902
Net Liabilities		
Net Liabilities at Beginning of Year	(672,118)	(489,256)
Net Operating Results	(6,851,023)	(6,126,652)
Net Financing Provided from General Revenues	6,783,290	5,943,790
	(739,851)	(672,118)
	$ 206,186	$ 268,784

The accompanying notes and schedules are part of these financial statements.

Office of the Information and Privacy Commissioner

Statement of Cash Flows

Year ended March 31, 2015

	2015	2014
Operating Transactions		
Net Operating Results	$ (6,851,023)	$ (6,126,652)
Non-cash Items Included in Net Operating Results		
Amortization of Tangible Capital Assets	83,876	56,556
Loss on Disposal of Tangible Capital Assets	-	-
	(6,767,147)	(6,070,096)
(Increase) Decrease in Accounts Receivable	(3,237)	3,153
Decrease (Increase) in Prepaid Expenses	610	(140)
Increase in Accounts Payable	5,135	271,486
Cash Applied to Operating Transactions	(6,764,639)	(5,795,597)
Capital Transactions		
Acquisition of Tangible Capital Assets	(18,651)	(148,193)
Financing Transactions		
Net Financing Provided From General Revenues	6,783,290	5,943,790
Cash, Increase (Decrease)	-	-
Cash, Beginning of Year	100	100
Cash, End of Year	$ 100	$ 100

The accompanying notes and schedules are part of these financial statements.

Financial Statements

Office of the Information and Privacy Commissioner

Notes to the Financial Statements

Year ended March 31, 2015

Note 1 Authority

The Office of the Information and Privacy Commissioner operates under the authority of the *Freedom of Information and Protection of Privacy Act*. The net cost of the operations of the Office is borne by the General Revenue Fund of the Province of Alberta. Annual operating budgets are approved by the Standing Committee on Legislative Offices.

Note 2 Purpose

The Office of the Information and Privacy Commissioner provides oversight on the following legislation governing access to information and protection of privacy:

Freedom of Information and Protection of Privacy Act
Health Information Act
Personal Information Protection Act

The major operational purposes of the Office of the Information and Privacy Commissioner are:

- To provide independent reviews of decisions made by public bodies, custodians and organizations under the Acts and the resolution of complaints under the Acts;
- To advocate protection of privacy for Albertans; and
- To promote openness and accountability for public bodies.

Note 3 Summary of Significant Accounting Policies and Reporting Practices

These financial statements are prepared in accordance with Canadian Public Sector Accounting Standards.

a) Reporting Entity

The reporting entity is the Office of the Information and Privacy Commissioner (the Office), for which the Information and Privacy Commissioner is responsible.

The Office operates within the General Revenue Fund (the Fund). The Fund is administered by the President of Treasury Board and Minister of Finance. All cash receipts of the Office are deposited into the Fund and all cash disbursements made by the Office are paid from the Fund. Net Financing provided from General Revenues is the difference between all cash receipts and all cash disbursements made.

b) Basis of Financial Reporting

Revenues

All revenues are reported on the accrual basis of accounting.

Expenses

Directly Incurred

Directly incurred expenses are those costs the Office has primary responsibility and accountability for, as reflected in the Office's budget documents.

In addition to program operating expenses such as salaries, supplies, etc., directly incurred expenses also include:

- Amortization of tangible capital assets;
- Pension costs, which are the cost of employer contributions for current service of employees during the year; and
- Valuation adjustments which represent the change in management's estimate of future payments arising from obligations relating to vacation pay.

Incurred by Others

Services contributed by other entities in support of the Office's operations are not recognized and are disclosed in Schedule 2.

Assets

Financial assets are assets that could be used to discharge existing liabilities or finance future operations and are not for consumption in the normal course of operations. Financial assets of the Office are limited to financial claims, such as receivables from other organizations.

Tangible capital assets of the Office are recorded at historical cost and are amortized on a straight-line basis over the estimated useful lives of the assets. The threshold for tangible capital assets is $5,000 except major enhancements to existing systems is $250,000 and new systems development is $100,000.

Office of the Information and Privacy Commissioner

Notes to the Financial Statements *(continued)*

Year ended March 31, 2015

Liabilities

Liabilities are recorded to the extent that they represent present obligations as a result of events and transactions occurring prior to the end of the fiscal year. The settlement of liabilities will result in sacrifice of economic benefits in the future.

Net Liabilities

Net liabilities represent the difference between the Office's liabilities and the carrying value of its assets.

Canadian Public Sector Accounting Standards require a "net debt" presentation for the statement of financial position in the summary financial statements of governments. Net debt presentation reports the difference between financial assets and liabilities as "net debt" or "net financial assets" as an indicator of the future revenues required to pay for past transactions and events. The Office operates within the government reporting entity, and does not finance all its expenditures by independently raising revenues. Accordingly, these financial statements do not report a net debt indicator.

Valuation of Financial Assets and Liabilities

Fair value is the amount of consideration agreed upon in an arm's length transaction between knowledgeable, willing parties who are under no compulsion to act.

The fair values of Cash, Accounts Receivable, Accounts Payable and Accrued Liabilities are estimated to approximate their carrying values because of the short term nature of these instruments.

c) Financial Instruments

As the Office does not have any transactions involving financial instruments that are classified in the fair value category and has insignificant foreign currency transactions, there are no remeasurement gains and losses and therefore a statement of remeasurement gains and losses has not been presented.

Office of the Information and Privacy Commissioner

Notes to the Financial Statements *(continued)*

Year ended March 31, 2015

Note 4 Tangible Capital Assets

	Office equipment and furniture	Computer hardware and software	Total
Estimated Useful Life	5-10 years	3-5 years	
Historical Cost			
Beginning of Year	$ 236,729	$ 413,935	$ 650,664
Additions	18,651	-	18,651
Disposals, Including Write-Downs	-	-	-
	$ 255,380	$ 413,935	$ 669,315
Accumulated Amortization			
Beginning of Year	$ 203,792	$ 179,127	$ 382,919
Amortization Expense	10,706	73,170	83,876
Effect of Disposals	-	-	-
	$ 214,498	$ 252,297	$ 466,795
Net Book Value at March 31, 2015	$ 40,882	$ 161,638	$ 202,520
Net Book Value at March 31, 2014	$ 32,937	$ 234,808	$ 267,745

Office of the Information and Privacy Commissioner

Notes to the Financial Statements *(continued)*

Year ended March 31, 2015

Note 5 Defined Benefit Plans

The Office participates in the multiemployer pension plans: Management Employees Pension Plan, Public Service Pension Plan and Supplementary Retirement Plan for Public Service Managers. The expense for these pension plans is equivalent to the annual contributions of $721,657 for the year ended March 31, 2015 (2014 - $601,047).

At December 31, 2014, the Management Employees Pension Plan reported a surplus of $75,805,000 (2013 surplus $50,457,000) and the Public Service Pension Plan reported a deficiency of $803,299,000 (2013 deficiency $1,254,678,000). At December 31, 2014, the Supplementary Retirement Plan for Public Service Managers had a deficiency of $17,203,000 (2013 deficiency $12,384,000).

The Office also participates in a multiemployer Long Term Disability Income Continuance Plan. At March 31, 2015, the Management, Opted Out and Excluded Plan reported an actuarial surplus of $32,343,000 (2014 - surplus $24,055,000). The expense for this plan is limited to employer's annual contributions for the year.

Note 6 Contractual Obligations

Contractual obligations are obligations of the Office to others that will become liabilities in the future when the terms of those contracts or agreements are met.

	2015	2014
Obligations under operating leases and contracts	$ 11,958	$ 26,356

Estimated payment requirements for each of the next three years are as follows:

	Total
2015-16	$ 8,812
2016-17	3,146
2017-18	-
	$ 11,958

Office of the Information and Privacy Commissioner

Notes to the Financial Statements *(continued)*

Note 7 Approval of Financial Statements

These financial statements were approved by the Information and Privacy Commissioner.

Schedule 1 - Salary and Benefits Disclosure

Year ended March 31, 2015

	2015				2014
	Base Salary [a]	Other Cash Benefits	Other Non-cash Benefits [b][c]	Total	Total
Senior Official					
Information and Privacy Commissioner	$ 197,672	$ -	$ 61,401	$ 259,073	$ 268,696

[a] Base salary includes pensionable base pay.
[b] Other non-cash benefits include the government's share of all employee benefits and contributions or payments made on behalf of employee, including pension, supplementary retirement plan, health care, dental coverage, group life insurance, short and long term disability plans, health spending account, conference fees, and professional memberships and tuition fees.
[c] Automobile provided. Taxable benefit amount included in other non-cash benefits.

Financial Statements

Office of the Information and Privacy Commissioner

Schedule 2 - Allocated Costs

Year ended March 31, 2015

	2015				2014
	Expenses - Incurred by Others				
Program	**Expenses [a]**	**Accommodation Costs [b]**	**Telephone Costs [c]**	**Total Expenses**	**Total Expenses**
Operations	$ 6,854,338	$ 452,934	$ 15,684	$ 7,322,956	$ 6,594,356

[a] Expenses - Directly Incurred as per Statement of Operations.
[b] Costs shown for Accommodation (includes grants in lieu of taxes), allocated by square meters.
[c] Telephone Costs is the line charge for all phone numbers.

Appendices

Appendix A: Cases Opened under FOIP, HIA, PIPA by Entity Type 68

Appendix B: Cases Closed under FOIP, HIA, PIPA by Entity Type 71

Appendix C: Orders, Decisions and Public Investigation Reports Issued 74

Appendix D: Accepted Privacy Impact Assessments by Public Body, Custodian and Organization Types 76

Appendix A: Cases Opened under FOIP, HIA, PIPA by Entity Type

Statistics are from the period of April 1, 2014 to March 31, 2015

FOIP Entity Type	Advice and Direction	Authorization to Disregard Request	Request Authorization to Indirectly Collect	Complaint	Disclosure to Commissioner	Notification to OIPC	Engage in or Commission a Study	Excuse Fees	Investigation Generated by Commissioner	Offence Investigation	Privacy Impact Assessment	Request for Information	Request for Review	Request for Review 3rd Party	Request Time Extension	Self-reported Breach	Total
Agencies	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Boards	0	1	0	5	0	0	0	0	0	0	0	0	23	1	8	0	38
Colleges	0	0	0	2	0	1	0	0	0	0	0	0	2	0	1	3	9
Commissions	0	0	0	0	0	0	0	0	0	0	1	0	9	2	1	1	14
Committees	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Crown Corporations	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1
Federal Departments	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Foundations	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Government Ministries/ Departments	0	2	0	20	1	0	0	6	20	0	6	12	104	3	40	6	220
Hospital Board (Covenant Health)	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1
Law Enforcement Agencies	0	1	0	7	0	1	0	0	1	0	0	1	48	0	0	0	59
Legislative Assembly Offices	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Local Government Bodies	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	2
Long Term Care Centres	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Municipalities	0	2	0	22	0	1	0	0	0	0	3	7	39	5	9	6	94
Nursing Homes	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1
Office of the Premier/ Alberta Executive Council	0	0	0	0	0	0	0	0	1	0	0	0	5	2	0	0	8
Officers of the Legislature	0	0	0	0	0	0	0	0	0	0	0	2	1	0	0	1	4
Panels	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Provincial Health Board (Health Quality Council)	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1
Regional Health Authorities (Alberta Health Services)	0	0	0	10	0	0	0	0	0	0	0	0	33	7	2	2	54
School Districts	0	0	0	15	0	3	0	0	1	0	2	0	10	0	0	17	48
Universities	0	1	0	3	0	2	0	0	0	0	0	1	13	2	2	2	26
Other	0	0	0	0	0	0	0	1	0	2	0	1	3	0	0	2	9
Total	**0**	**7**	**0**	**85**	**1**	**8**	**0**	**7**	**23**	**2**	**12**	**24**	**294**	**22**	**63**	**41**	**589**

Note: The statistics do not include intake cases

Appendix A: Cases Opened under FOIP, HIA, PIPA by Entity Type

Statistics are from the period of April 1, 2014 to March 31, 2015

HIA Entity Type	Advice and Direction	Authorization to Disregard Request	Complaint	Notification to OIPC	Engage in or Commission a Study	Excuse Fees	Investigation Generated by Commissioner	Offence Investigation	Privacy Impact Assessment	Request for Information	Request for Review	Request Time Extension	Self-reported Breach	Total
Affiliates and Information Managers (Electronic Medical Record Vendors/Physician Office System Program, Consultants)	0	0	0	0	0	0	1	0	1	3	0	0	0	5
Associations, Boards, Councils, Committees, Commissions, Panels or Agencies, created by Custodians	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Chiropractors	0	0	1	0	0	0	0	0	24	0	0	0	2	27
Dental Hygienists	0	0	0	0	0	0	0	0	2	0	0	0	0	2
Dentists	0	0	0	0	0	0	0	0	0	2	0	0	0	2
Denturists	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Government Ministries/Departments	0	0	0	0	0	0	0	0	1	0	0	0	0	1
Health Professional Colleges and Associations	0	0	0	0	0	0	0	0	0	3	0	0	1	4
Hospital Board (Covenant Health)	0	0	4	0	0	0	2	0	2	0	1	0	0	9
Long Term Care Centres	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Midwives	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Minister of Health	0	0	1	0	0	0	0	0	18	1	1	0	1	22
Nursing Homes	0	0	0	0	0	0	0	0	0	0	1	0	1	2
Opticians	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Optometrists	0	0	0	0	0	0	0	0	1	0	0	0	0	1
Pharmacies/Pharmacists	0	0	4	0	0	0	5	0	83	0	0	0	4	96
Physicians	0	1	9	0	0	1	11	0	145	5	4	0	28	204
Primary Care Networks	0	0	0	0	0	0	0	0	8	2	0	0	5	15
Provincial Health Board (Health Quality Council)	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Regional Health Authorities (Alberta Health Services)	0	0	20	0	0	0	9	0	26	0	9	0	31	95
Registered Nurses	0	0	0	0	0	0	0	0	29	2	0	0	0	31
Researchers	0	0	0	0	0	0	0	0	0	1	0	0	1	2
Research Ethics Boards	0	0	0	0	0	0	0	0	0	1	0	0	0	1
Subsidiary Health Corporations	0	0	0	0	0	0	0	0	1	0	0	0	2	3
Universities/Faculties of Medicine	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	2	0	4	0	0	0	6
Total	**0**	**1**	**39**	**0**	**0**	**1**	**28**	**2**	**341**	**24**	**16**	**0**	**76**	**528**

Note: The statistics do not include intake cases.

Appendix A: Cases Opened under FOIP, HIA, PIPA by Entity Type

Statistics are from the period of April 1, 2014 to March 31, 2015

PIPA Entity Type	Advice and Direction	Authorization to Disregard Request	Complaint	Notification to OIPC	Engage in or Commission a Study	Excuse Fees	Investigation Generated by Commissioner	Offence Investigation	Privacy Impact Assessment	Request for Information	Request for Review	Request Time Extension	Request for Advance Ruling	Self-reported Breach	Total
Accommodation & Food Services	0	0	2	0	0	0	1	0	0	0	2	0	0	3	8
Admin & Support Services	0	0	3	0	0	0	0	0	0	0	2	0	0	4	9
Arts, Entertainment & Recreation	0	0	1	0	0	0	0	0	0	1	1	0	0	0	3
Child Day-Care Services	0	0	3	0	0	0	0	0	0	1	3	0	0	3	10
Construction	0	0	4	0	0	0	0	0	0	0	2	0	0	0	6
Credit Unions	0	0	0	0	0	0	0	0	0	0	0	0	0	35	35
Dealers in Automobiles	0	0	1	0	0	0	1	0	0	0	2	0	0	1	5
Educational Services	0	0	2	0	0	0	1	0	0	0	0	0	0	1	4
Finance	0	0	3	0	0	0	0	0	0	0	1	0	0	10	14
Information & Cultural Industries	0	0	7	0	0	0	1	0	0	0	1	0	0	8	17
Insurance Industry	0	0	5	0	0	0	1	0	1	1	2	0	0	19	29
Legal Services	0	0	11	0	0	0	0	0	0	0	1	0	0	3	15
Management of Companies and Enterprises	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
Manufacturing	0	0	1	0	0	0	0	0	0	0	0	0	0	5	6
Mining, Oil and Gas	0	0	5	0	0	0	0	0	0	0	8	0	0	3	16
Private Health Care & Social Assistance	0	0	8	0	0	0	0	0	0	0	6	0	0	10	24
Professional, Scientific & Technical	0	0	3	0	0	0	0	0	1	0	0	0	0	2	6
Public Administration	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
Real Estate, Rental, Leasing	0	0	26	0	0	0	0	0	0	0	3	0	0	1	30
Retail	0	0	7	0	0	0	1	0	0	1	1	0	0	11	21
Trades/Contractors	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1
Transportation	0	0	3	0	0	0	0	0	0	0	1	0	0	2	6
Utilities	0	0	3	0	0	0	0	0	0	0	1	0	0	1	5
Wholesale Trade	0	0	3	0	0	0	0	0	0	0	0	0	0	2	5
Other	0	0	20	0	0	0	1	0	1	5	14	1	0	12	54
Total	**0**	**0**	**121**	**0**	**0**	**0**	**7**	**0**	**3**	**9**	**52**	**1**	**0**	**138**	**331**

Note: The statistics do not include intake cases

Appendix B: Cases Closed under FOIP, HIA, PIPA by Entity Type

Statistics are from the period of April 1, 2014 to March 31, 2015

FOIP Entity Type	Advice and Direction	Authorization to Disregard Request	Request Authorization to Indirectly Collect	Complaint	Disclosure to Commissioner	Notification to OIPC	Engage in or Commission a Study	Excuse Fees	Investigation Generated by Commissioner	Offence Investigation	Privacy Impact Assessment	Request for Information	Request for Review	Request for Review 3rd Party	Request Time Extension	Self-reported Breach	Total
Agencies	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Boards	0	0	0	6	0	0	0	1	0	0	1	1	7	0	8	1	25
Child and Family Service Authorities	0	0	0	3	0	0	0	0	1	0	0	0	0	0	0	0	4
Colleges	0	0	0	2	0	1	0	0	0	0	0	0	2	0	1	2	8
Commissions	0	0	0	1	0	0	0	0	0	0	0	0	3	2	1	0	7
Committees	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Crown Corporations	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0	2
Federal Departments	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Foundations	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Government Ministries/ Departments	0	2	0	62	0	0	0	5	3	0	10	15	96	3	41	5	242
Hospital Board (Covenant Health)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Law Enforcement Agencies	0	1	0	10	0	1	0	1	1	0	0	0	30	0	0	0	44
Legislative Assembly Offices	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Local Government Bodies	0	0	0	1	0	0	0	1	0	0	0	0	1	0	0	0	3
Long Term Care Centres	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1
Municipalities	0	1	0	10	0	1	0	11	0	0	2	7	33	7	9	5	86
Nursing Homes	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Office of the Premier/ Alberta Executive Council	0	0	0	0	0	0	0	0	0	0	0	0	12	0	0	0	12
Officers of the Legislature	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	2	4
Panels	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Provincial Health Board (Health Quality Council)	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1
Regional Health Authorities (Alberta Health Services)	0	0	0	5	0	0	0	2	0	0	1	0	27	11	2	1	49
School Districts	0	0	0	13	0	3	0	0	0	0	1	2	7	0	0	7	33
Universities	0	0	0	3	0	2	0	1	2	0	1	1	8	1	2	2	23
Other	0	0	0	0	0	0	0	2	0	0	0	1	2	0	0	1	6
Total	**0**	**4**	**0**	**117**	**0**	**8**	**0**	**25**	**7**	**0**	**16**	**29**	**230**	**24**	**64**	**26**	**550**

Note: The statistics do not include intake cases.

Appendix B: Cases Closed under FOIP, HIA, PIPA by Entity Type

Statistics are from the period of April 1, 2014 to March 31, 2015

HIA

Entity Type	Advice and Direction	Authorization to Disregard Request	Complaint	Notification to OIPC	Engage in or Commission a Study	Excuse Fees	Investigation Generated by Commissioner	Offence Investigation	Privacy Impact Assessment	Request for Information	Request for Review	Request Time Extension	Self-reported Breach	Total
Affiliates and Information Managers (Electronic Medical Record Vendors/Physician Office System Program, Consultants)	0	0	0	0	0	0	1	0	0	2	0	0	1	4
Associations, Boards, Councils, Committees, Commissions, Panels or Agencies, created by Custodians	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Chiropractors	0	0	1	0	0	0	0	0	20	0	0	0	2	23
Dental Hygienists	0	0	0	0	0	0	0	0	1	0	0	0	0	1
Dentists	0	0	2	0	0	0	0	0	0	2	0	0	0	4
Denturists	0	0	0	0	0	0	0	0	0	0	0	0	1	1
Government Ministries/Departments	0	0	0	0	0	0	0	0	1	0	0	0	0	1
Health Professional Colleges and Associations	0	0	0	0	0	0	0	0	0	2	0	0	1	3
Hospital Board (Covenant Health)	0	0	2	0	0	0	0	0	5	2	0	0	0	9
Long Term Care Centres	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Midwives	0	0	0	0	0	0	0	0	16	0	0	0	0	16
Minister of Health	0	0	0	0	0	0	0	0	18	2	1	0	3	24
Nursing Homes	0	0	0	0	0	0	0	0	0	0	0	0	1	1
Opticians	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Optometrists	0	0	0	0	0	0	0	0	1	0	0	0	0	1
Pharmacies/Pharmacists	0	0	3	0	0	0	1	0	73	0	0	0	2	79
Physicians	0	1	21	0	0	0	12	0	121	7	5	0	31	198
Primary Care Networks	0	0	0	0	0	0	0	0	13	2	0	0	7	22
Provincial Health Board (Health Quality Council)	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Regional Health Authorities (Alberta Health Services)	0	0	8	0	0	0	3	0	38	0	3	0	19	71
Registered Nurses	0	0	0	0	0	0	0	0	31	0	0	0	0	31
Reseachers	0	0	0	0	0	0	0	0	0	0	0	0	1	1
Research Ethics Boards	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Subsidiary Health Corporations	0	0	5	0	0	0	1	1	2	0	0	0	2	11
Universities/Faculties of Medicine	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	0	0	0	0	0	0	0	0	2	0	0	0	2
Total	**0**	**1**	**42**	**0**	**0**	**0**	**18**	**1**	**340**	**21**	**9**	**0**	**71**	**503**

Note: The statistics do not include Intake cases

Appendix B: Cases Closed under FOIP, HIA, PIPA by Entity Type

Statistics are from the period of April 1, 2014 to March 31, 2015

PIPA Entity Type	Advice and Direction	Authorization to Disregard Request	Complaint	Notification to OIPC	Engage in or Commission a Study	Excuse Fees	Investigation Generated by Commissioner	Offence Investigation	Privacy Impact Assessment	Request for Information	Request for Review	Request for Review 3rd Party	Request Time Extension	Request Advanced Ruling	Self-reported Breach	Total
Accommodation & Food Services	0	0	5	0	0	0	1	0	0	0	0	0	0	0	0	6
Admin & Support Services	0	0	1	0	0	0	0	0	0	0	1	0	0	0	2	4
Arts, Entertainment & Recreation	0	0	3	0	0	0	0	0	0	1	0	0	0	0	1	5
Child Day-Care Services	0	0	2	0	0	0	0	0	0	1	0	0	0	0	3	6
Collection Agencies	0	0	3	0	0	0	0	0	0	0	0	0	0	0	1	4
Construction	0	0	6	0	0	0	0	0	0	0	4	0	0	0	0	10
Credit Bureaus	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
Dealers in Automobiles	0	0	6	0	0	0	0	0	0	0	2	0	0	0	0	8
Educational Services	0	0	1	0	0	0	0	0	0	0	2	0	0	0	3	6
Finance	0	0	5	0	0	0	0	0	0	0	2	0	0	0	21	28
Health care and social assistance	0	0	5	0	0	0	0	0	0	0	3	0	0	0	2	10
Information & Cultural Industries	0	0	8	0	0	0	2	0	0	0	3	0	0	0	3	16
Insurance Industry	0	0	6	0	0	0	0	0	1	0	3	0	0	0	15	25
Legal Services	0	1	3	0	0	0	0	0	0	0	2	0	0	0	1	7
Manufacturing	0	0	2	0	0	0	0	0	0	0	1	0	0	0	2	5
Medical & Diagnostic Laboratories	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1
Mining, Oil and Gas	0	1	4	0	0	0	0	0	0	0	3	0	0	0	2	10
Nursing Homes/Home Health Care	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
Professional, Scientific & Technical	0	0	1	0	0	0	0	0	2	1	0	0	0	0	1	5
Real Estate, Rental, Leasing	0	0	23	0	0	0	9	0	0	0	0	0	0	0	1	33
Retail	0	0	12	0	0	0	0	0	0	1	2	0	0	0	7	22
Trades/Contractors	0	0	1	0	0	0	0	0	0	0	2	0	0	0	0	3
Transportation	0	0	1	0	0	0	0	0	0	0	3	0	0	0	1	5
Utilities	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	3
Wholesale Trade	0	0	1	0	0	0	0	0	0	0	0	0	0	0	3	4
Other	0	0	11	0	0	0	0	0	0	2	11	0	1	0	5	30
Total	**0**	**2**	**114**	**0**	**0**	**0**	**12**	**0**	**3**	**6**	**44**	**0**	**1**	**0**	**76**	**258**

Note: The statistics do not include Intake cases.

Appendix C: Orders and Public Investigation Reports Issued

Statistics are from the period April 1, 2014 to March 31, 2015

FOIP RESPONDENT	ORDERS	DECISIONS	PUBLIC INVESTIGATION REPORTS	TOTAL
Alberta Education	0	0	1	1
Alberta Energy Regulator	1	0	0	1
Alberta Health	7	1	0	8
Alberta Health Services	4	1	0	5
Alberta Human Services	3	0	0	3
Alberta Jobs, Skills, Training and Labour	0	1	0	1
Alberta Justice & Solicitor General	7	2	0	9
Alberta Transportation	1	0	0	1
Alberta Treasury Board and Finance	1	0	0	1
Appeals Commission for Alberta Workers' Compensation	1	0	0	1
Bow Valley College	1	0	0	1
Calgary Board of Education	1	0	0	1
Calgary Police Service	4	0	0	4
Calgary Regional Partnership	0	1	0	1
City of Calgary	2	0	0	2
City of Cold Lake	1	0	0	1
City of Lethbridge	1	0	0	1
City of St. Albert	1	0	0	1
County of Thorhild No. 7	1	0	0	1
Edmonton Police Service	4	0	0	4
Medicine Hat Police Commission	1	0	0	1
Town of Sylvan Lake	1	0	0	1
Workers' Compensation Board	2	0	0	2
Sub-Total	**45**	**6**	**1**	**52**

HIA RESPONDENT	ORDERS	DECISIONS	PUBLIC INVESTIGATION REPORTS	TOTAL
Alberta Health	1	0	0	1
Alberta Health Services	1	0	0	1
Medicentres Canada Inc.	0	0	1	1
Sub-Total	**2**	**0**	**1**	**3**

PIPA RESPONDENT	ORDERS	DECISIONS	PUBLIC INVESTIGATION REPORTS	TOTAL
Canadian Corps of Commissionaires	1	0	0	1
CDN Power Pac Mechanical/Electric Inc.	1	0	0	1
Consumer Choice Awards	1	0	0	1
Crawford & Company (Canada) Inc.	1	0	0	1
Storybook Theatre Society, and Morpheus Theatre Society	1	0	0	1
TD Insurance	1	0	0	1
Sub-Total	**6**	**0**	**0**	**6**
Total	**53**	**6**	**2**	**61**

FOIP Orders: 45 (63 cases)
FOIP Decisions: 6 (10 cases)
FOIP Investigation Reports: 1 (35 cases)

HIA Orders: 2 (2 cases)
HIA Decisions: 0
HIA Investigation Reports: 1 (24 cases)

PIPA Orders: 6 (8 cases)
PIPA Decisions: 0
PIPA Investigation Reports: 0

Notes: A single Order, Decision or Investigation Report can relate to more than one entity and more than one file.

The number of Orders, Decisions and Investigation Reports are counted by the number of Order, Decision or Investigation Report numbers assigned.

Orders and Decisions are recorded by the date the Order or Decision was signed, rather than the date the Order or Decision was publicly released. Investigation Reports are recorded by the date they were publicly issued.

A copy of all Orders, Decisions and Public Investigation Reports are available on the OIPC web site: www.oipc.ab.ca.

Appendix D: Accepted Privacy Impact Assessments by Public Body, Custodian and Organization Types

Statistics are from the period April 1, 2014 to March 31, 2015

PUBLIC BODY	PIA TITLE
BOARDS	
Workers' Compensation Board	CLEAR (Claim and Employer Account Registry)
MINISTRIES/DEPARTMENTS	
Education	Teacher Worplace Information System (TWINS)
	Corporate Data Warehouse (CDW) Technology Refresh Project
Human Services	Child and Youth Data Lab (CYDL) - Project Two (F7997)
	Child and Youth Data Lab (CYDL) - Project Two (H6146)
Infrastructure	Draft - Online Parking Request and Administration System (OPRA)
Jobs, Skills, Training and Labour	Occupational Health and Safety Blood Lead Tracking Project (BLT)
Justice and Solicitor General	Integrated Justice Services Project - Safe Communities Resource Centre
Service Alberta	MyAlberta Digital Identity Program
MUNICIPALITIES	
Strathcona County	Fire Station 6 Surveillance
Town of Coaldale	Privacy Impact Assessment – Town of Coaldale
REGIONAL HEALTH AUTHORITIES	
Alberta Health Services	Staff Scheduling Application
SCHOOL DISTRICTS	
Northern Lights School Division #69	Electronic Student Records Project
UNIVERSITIES	
Mount Royal University	Google Apps for Education Application

CUSTODIAN	PIA TITLE
CHIROPRACTORS	
Dr. Andrea Sargent	Cliniko
Dr. Ayesha Ebrahim	ChiroSUITE Vendor: Sunbaked Software Inc.
Dr. Brett Hill, Chiropractor	ClinicKeeper for Chiropractors
Dr. Dale Macdonald	ChiroSuite Electronic Medical Records
Dr. Dave Phillips	ChiroSuite v5 Electronic Record System
Dr. David Fullerton	ChiroSuite v5
Dr. David Linford	ChiroSuite v5 Electronic Patient Record System
Dr. Derek Lampshire	River Valley Health Electronic Records Project: Amendment for addition of RVH Performance
Dr. Genevieve Ford	Atlas Chiropractic System Local Implementation and Netcare
Dr. Gregory P. Uchacz	ChiroSuite v5 Electronic Patient Record System
Dr. Jeffrey Scholten	ChiroSUITE
Dr. Kent Stuber	Organizational Privacy Management - Electronic Medical Records
Dr. Manjit S. Gauba	Chiro Touch Practice Management Electronic Medical Records Implementation and Netcare
Dr. Ryan Hoover	MRX Solutions ChartMaster
Dr. Ryan MacDonald	Practice Perfect Electronic Medical Records + Management Software
Dr. Todd Halowski	Visitbase Practice Management Software
Dr. Todd Lynes	Electronic Medical Records
Dr. Travis W. M. Cox	Atlas Chiropractic System
Dr. Troy Samchuk	ChiroSuite v5 Electronic Patient Record System

CUSTODIAN	PIA TITLE
HOSPITAL BOARDS	
Covenant Health	Covenant Health's Organizational Privacy Management
	eCritical MetaVision System
	Grey Nuns Emergency Services Patient Care Model
	Kroll Outpatient Pharmacy Information System (Lethbridge)
	Pulmonary Function Results to Netcare
MIDWIVES	
Ms. Gaelyn Anderson	Full Organizational Submission
Ms. Barbara Bodiguel	Full Organizational Submission - Blessing Way Midwifery
Ms. Barbara Scriver	Organization Management and Organization Information Management
Ms. Cathy Harness	Full Organizational Submission - Joyspring Midwifery
Ms. Heidi Coughlin	Full Organizational Submission - HOPE Midwives
Ms. Helen Cotter	Electronic Medical Records (EMR) to: Organization Management and Organization Information Management
Ms. Jennifer Bindon	Full Organizational Submission -Prairie Midwives
Ms. Joan Margaret Laine	Organization Management and Organization Information Management
Ms. Kerstin Gafvels	Electronic Medical Records (EMR) to: Organization Management and Organization Information Management
Ms. Kimberley Schmidt	Full Organizational Submission - Aurora Midwives
Ms. Marie Wilkinson	Full Organizational Submission - Foothills
Ms. Maura Burns	Electronic Medical Records (EMR) to: Organization Management and Organization Information Management
Ms. Noreen Walker	Organizational Management and Organization Information Management
Ms. Sharyne Fraser	Electronic Medical Records (EMR) to: Organization Management and Organization Information Management
Ms. Shianna Pace	Electronic Medical Records (EMR) to: Organization Management and Organization Information Management
Ms. Vivian MacLean	Organization Management and Organization Information Management

CUSTODIAN	PIA TITLE
MINISTRY OF HEALTH	
Alberta Health	Addendum 2: Alberta Cancer Registry (ACR) - Update to ACR Data Sharing
	Alberta Blue Cross (ABC) Non-Group Coverage Billing Transfer Addendum 1
	Alberta Organ and Tissue Donation Registry (AOTDR)
	Alberta Organ and Tissue Donation Registry (AOTDR)
	Alberta Organ and Tissue Donation Registry (AOTDR) - Addendum 2
	CD/OM (Communicable Disease-Outbreak Management) - Data Transfer to Alberta Health: Addendum 1 - AHS Release 1.x and Interim Access Process
	Management of Duplicate Claims Submitted to the WCB and the Alberta Health Care Incurance Plan (AHCIP) - Addendum 1
	Newborn Metabolic Screening (NMS)
	Pharmaceutical Information Network (PIN) Addendum 7
	Public Health and Surveillance - Addendum 5: Community Health Assessment Survey (CHAS)
	Public Health and Surveillance - Addendum 6: Alberta Health Services Influenza Immunization
	Public Health and Surveillance - Addendum 7: Perinatal Outcomes
	Public Health and Surveillance - Addendum 4: Alberta Congenital; Anomalies Surveillance System (ACASS)
	Public Health and Surveillance - Addendum 8: Provincial Surveillance Initiative (PSI) Phase 1 - Release 1
	Third Addendum to the Provincial Personal Health Identifier (PHHI)/Person Directory (PD)
OPTOMETRISTS	
Dr. Ellen Anderson Penno	Full Organizational Submission with QSP Vendor Electronic Medical Records System - Western Laser Eye

CUSTODIAN	PIA TITLE
PHARMACIES/PHARMACISTS	
	60 Alberta Netcare PIAs
Castledowns Drug Centre	Kroll Pharmacy Practice Management System & Real-time Integration with PIN Pharmacists
Drayton Valley Value Drug Mart	Kroll Pharmacy Practice Management System & Real-time Integration with PIN encompassing: Netcare Access
Lemarchand Dispensary	Kroll Pharmacy Practice Management System & Real-time Integration with PIN
Life Med Pharmacy	Kroll Pharmacy Practice Management System and Real-time Integration with PIN
Loblaw Companies Limited	Pharmacy Central Reporting - Additional Modules
Meridian Pharmacy	Kroll V9 Kroll Pharmacy Practice Management System
Mr. Chad Rieger, Pharmacists	Immunization Program
Provost IDA	Kroll Pharmacy Practice Management System & Real-time Integration with PIN
Saddle Lake Pharmacy	Kroll Pharmacy Practice Management System & Real-time Integration with PIN.
Tawa Pharmasave	Kroll Pharmacy Practice Management System & Real-time Integration with PIN
The Medicine Shoppe #185	Kroll Pharmacy Practice Management System & Real-time Integration with PIN
Turtle Mountain Pharmacy Ltd.	Kroll V9 Pharmacy Practice Management System & Real-time Integration with PIN
PHYSICIANS	
	9 Alberta Netcare PIAs
Dr. A. Ebaij	Healthquest Electronic Medical Records encompassing: Netcare Access, Wireless, and Paper to QSP ASP Hosted Solution
Dr. Adeb Zayani	Microquest Healthquest local install Electronic Medical Records implementation encompassing: new clinic implementing QSP ASP Hosted Solution, and Physician Netcare Access
Dr. Adekunle Adegbulu	Telin Mediplan encompassing: organizational practices and reporting on information management systems
Dr. Adele Freeman	Alberta Netcare and PCN Participation: Calgary Foothills
Dr. Ahmed H. Abubaker El khazmy, Rimrock Medical Clinic	Microquest Healthquest Electronic Medical Records local install encompassing: Alberta Netcare
Dr. Aimen Fateis	Healthquest Electronic Medical Records encompassing: Alberta Netcare and PCN participation: Edmonton North
Dr. Angelina Lutwinski	QHR Technologies Accuro Electronic Medical Records encompassing: new clinic implementing ASP Hosted Solution and Physician Netcare Access

CUSTODIAN	PIA TITLE
Dr. Anshia van Jaarsveld	Merit Medical Clinic Electronic Medical Records implementation
Dr. Anwer Abdalla	Healthquest Electronic Medical Records local implementation encompassing: Alberta Netcare and PCN participation: Edmonton Southside
Dr. Aporna Kali	TELUS Health Solutions Wolf Electronic Medical Records encompassing: Data Migration, Wireless, QSP local install to QSP hosted EMR, Physician Netcare Access, and PCN participation: Grande Prairie
Dr. Awatif Elsiddeig	Microquest Healthquest Electronic Medical Records encompassing: Alberta Netcare and PCN participation: Edmonton Oliver
Dr. Ayesha Imran	TELUS Health Solutions Wolf Electronic Medical Records encompassing: Organizational Practice Reporting of Information Management Systems and PCN participation: Mosaic
Dr. Ayman Tadros, Mountain View Medical Clinic	QHR Technologies Accuro Electronic Medical Records encompassing: new clinic implementing QSP ASP Hosted Solution, Data Migration, Physician Netcare Access, and PCN Participation: South Calgary
Dr. B. Wayne Chang	TELUS Health Solutions - South Calgary Medical Clinic (Patient Portal) encompassing: PCN Participation: South Calgary
Dr. Bao Dang	Amended: Peak Medical and Peak Pulmonary Function Laboratories
Dr. Bao Dang	TELUS Physician Solutions
Dr. Chika Odunze	TELUS Health PS EMR Organization Management and ASP Hosted EMR encompassing: new clinic implementing QSP ASP Hosted Solution, Data Migration, Physician Netcare Access and PCN Participation: South Calgary
Dr. Christin Hilbert	TELUS Health Solutions Electronic Medical Records encompassing: PCN participation: Calgary West
Dr. Christine Kyriakides	TELUS Health Solutions Med Access
Dr. Christine Luelo	TELUS Health Solutions and Med Access Electronic Medical Records
Dr. David S. McDonald	TELUS Health Solutions encompassing: paper to ASP Hosted Solution and Wireless
Dr. Denis R. J. Vincent	ezReferral encompassing: Netcare Access and PCN participating in the Edmonton Southside
Dr. Devin Pugsley, Urology	TELUS Health Solutions Med Access encompassing: new clinic implementing QSP ASP Hosted Solution, Wireless and Physician Netcare Access
Dr. Doug Caine	Organization Management and Alberta Netcare
Dr. Eric Huang	Optimed Accuro 3 Electronic Medical Records encompassing: Non-QSP to QSP ASP Hosted Solution and Physician Netcare Access
Dr. Grant Campbell	Optimed Accuro encompassing: new clinic implementing QSP ASP Hosted Solution, Data Migration, Netcare Access, and PCN participation: Edmonton Oliver

CUSTODIAN	PIA TITLE
Dr. Gustavo Nogareda	Alberta Netcare encompassing: Paper patients records, and Wireless
Dr. Guy J. Lavoie	eHealth Vault implementation
Dr. H. Singh	TELUS Health Solutions Wolf Electronic Medical Records encompassing: new clinic implementing QSP ASP Hosted Solution, Wireless, Netcare Access, and PCN participation: Mosaic
Dr. Hazem Abushwereb	Healthquest Electronic Medical Records encompassing: Netcare Access and PCN Participation: Edmonton North
Dr. Hester Angenessa Gordon	TELUS Health Solutions Wolf ASP hosted EMR Solution encompassing: Organization Management, new clinic implementing ASP Hosted EMR Solution, Non-ASP to ASP Hosted EMR Solution (via paper charts), Data Migration, Physician Netcare Access and PCN Participation: Lakeland
Dr. Inderpreet Rai, Glenwood Medical Clinic	Amendment: F12 Networks implementation and Alberta Netcare Portal
Dr. Inderpreet Rai, Granville Medical Clinic	F12 Networks implementation and Alberta Netcare Vendor: TELUS Health Med Access PCN Participation: Edmonton West
Dr. Indrepreet Rai	F12 Networks implementation and Alberta Netcare Vendor: TELUS Health Med Access
Dr. J. Gusdal	Justik Medical Clinic Remote Access Project
Dr. J. Kenneth Lipinski	INTELERAD encompassing: Netcare Access
Dr. Jake Tremblay	University Wellness Services Counselling & Clinical Services Titanium Software System Electronic Medical Records
Dr. James N. Wolfli	Microquest Healthquest encompassing: new clinic implementing QSP ASP Hosted Solution, Data Migration and Physician Netcare Access
Dr. Jane Ballantine	Amendment: Policies and Procedures
Dr. Johann van der Merwe	Accuro Electronic Medical Records QHR encompassing: Organizational Privacy Management, Netcare Access and PCN participation: Calgary West
Dr. Joma Kondi	Microquest Healthquest Electronic Medical Records encompassing: Paper to QSP ASP Hosted Solution, Physician Netcare Access, and PCN participation: Edmonton North
Dr. Joseph Bergman	QHR Technologies Accuro Electronic Medical Records encompassing: new clinic implementing QSP ASP Hosted Solution and Physician Netcare Access
Dr. Josuha Thambiraj	Microquest Healthquest Electronic Medical Records encompassing: PCN participation: Edmonton West
Dr. K. Hennig	Microquest Electronic Medical Records encompassing: Netcare Access
Dr. Kar-Wing Cheung	Med Access Electronic Medical Records encompassing: new clinic implementing QSP ASP Hosted Solution, Data Migration, Wireless, Physician Netcare Access, and PCN participation: South Edmonton

CUSTODIAN	PIA TITLE
Dr. Kay Laverty	Healthquest Electronic Medical Records
Dr. Keith L. McNicol	Westview Physician Collaborative (WPC) Primary Care Data Management, Measurement & Reporting (PC-DMMR) System enpassing: Paticipation in the CPCSSN research initiative
Dr. Kim Derouin	TELUS Health Solutions Wolf Electronic Medical Records encompassing: new clinic implementing QSP ASP Hosted Solution, Data Migration, Wireless, Physician Netcare Access, and PCN participation: Red Deer
Dr. Kusai Abuhamed, Old Scona Medical Centre	Microquest Healthquest local install EMR implementation Old Scona Medical Centre to encompass: Alberta Netcare Access and PCN Participation: Edmonton Oliver
Dr. Laurie Lemieux	Full Organizational Submission encompassing: Netcare
Dr. Liane Belland	Accuro ASP Electronic Medical Records
Dr. Lily Toma	Organization Management and Organization Information Management and Alberta Netcare to encompass: Organizational Practices and Reporting on Information Management Systems and/or External Services in use. Vendor: Telin Mediplan EMR PCN Participation: Calgary Foothills
Dr. Lorne M. Zuk	Organization Management encompassing: Paper Patient Records and Physician Netcare Access
Dr. M. Gaas	Microquest Electronic Medical Records encompassing: implementation of QSP ASP Hosted Solution, Wireless, Physician, Netcare Access, PCN participation: South Edmonton
Dr. M. Muneer	TELUS Health Soultions Wolf Electronic Medical Records encompassing: new clinic implementing QSP ASP Hosted Solution and Netcare Access
Dr. Mahamad Bulk	Microquest Healthquest Electronic Medical Records encompassing: Netcare Access and PCN Participation: Edmonton Southside
Dr. Maher Jerudi	Microquest Healthquest Electronic Medical Records encompassing: Organization Management and Alberta Netcare
Dr. Mareli Powell	Med Access Electronic Medical Records encompassing: Netcare Portal
Dr. Mary Gawlinski	Odyssey Travel and Tropical Medicine Clinic
Dr. Michael Ashenhurst	TELUS Health Solutions Wolf Electronic Medical Records encompassing: Organizational Practices and Reporting on Information Management Systems and/or External Services in use
Dr. Michael Curtis Johnson	Accuro Electronic Medical Records local install encompassing: Organization Management and Alberta Netcare
Dr. Moises Lasaleta	Amendment: Addition of new clinic - Scenic Acres Medical Centre
Dr. Moizali Ramji	TELUS Health Solutions Wolf Electronic Medical Records encompassing: Alberta Netcare and PCN Participation: Sherwood Park
Dr. Oladipo Odubanjo	TELUS Health Solutions Wolf Electronic Medical Records encompassing: PCN participation: Highland

CUSTODIAN	PIA TITLE
Dr. Olufemi Adekey	Microquest Healthquest Electronic Medical Records encompassing: Organizational Practices and Reporting on Information Management Systems and/or External Services in use, and PCN participation: Grande Prairie
Dr. Paul A. Lubitz	Microquest Healthquest Electronic Medical Records encompassing: new clinic implementing QSP ASP Hosted Solution, Paper to QSP ASP Hosted Solution, and Netcare Access
Dr. Paul G.R. Whidden	Organization Management and Organization Information Management encompassing: Alberta Netcare
Dr. Paul Schembri	Microquest Healthquest Electronic Medical Records encompassing: QSP local install to QSP hosted EMR, and Physician Netcare Access
Dr. Ralph Sinn	Organization Management
Dr. Raymond Lai	Disaster Recovery Site (DRS)
Dr. Raymond Lai	Electronic Billing
Dr. Raymond Lee	Organization Management and Alberta Netcare encompassing: paper patient record, Wireless, and PCN participation: Edmonton West
Dr. Reda Essa	Microquest Healthquest Electronic Medical Records local install encompassing: new clinic implementing QSP ASP Hosted Solution, Paper to QSP ASP Hosted Solution, Data Migration, Wireless, and Physician Netcare Access
Dr. Robert Hauptman, Pain Consulting Clinic	Organizational Privacy Management and Electronic Medical Records System
Dr. Ronald J. Brown	QHR Accuro Electronic Medical Records
Dr. Ronald ML Young	Med Access Electronic Medical Records encompassing: Organizational Practices, Reporting on Information and Management Systems and/or External Services, VCUR 2008 ASP hosted EMR, and Netcare Access
Dr. Ruan van Rooyen	TELUS Health Solutions Wolf ASP hosted Electronic Medical Records Solution encompassing: new clinic implementing QSP ASP Hosted Solution, Data Migration, Wireless, Physician Netcare Access and PCN participation: Lakeland
Dr. S.A. Jansen van Rensburg	Optimed Electronic Medical Records encompassing: Netcare Access
Dr. Sameer Qureshi	TELUS Health Soultions Wolf Electronic Medical Records encompassing: new clinic implementing QSP ASP Hosted Solution, Data Migration, Wireless, POSP Physician Netcare Access, and PCN participation: Mosaic
Dr. Samir Mouhammed	Healthquest Electronic Medical Records encompassing: Organizational Privacy Management and PCN participation: Edmonton West
Dr. Sean Grodin	UCMG Billing Services

CUSTODIAN	PIA TITLE
Dr. Sean Grondin	eScription
Dr. Shabbir Hassan	TELUS Health Solutions Wolf Electronic Medical Records encompassing: Alberta Netcare
Dr. Sherif El-Maadawy	Microquest Healthquest Electronic Medical Records local install encompassing: new clinic implementing QSP ASP Hosted Solution, Paper records to local install EMR Hosted Solution, Data Migration, Wireless, Physician Netcare Access, and PCN participation: Edmonton West
Dr. Stephen Miller	Organization Management and Alberta Netcare
Dr. Stephen R. Fugler	F12 Networks Electronic Medical Records/ Microquest Healthquest encompassing: Data Migration, and PCN participation: Wolf Creek
Dr. Suhaib Alkurtass	Healthquest Electronic Medical Records encompassing: Organizational Management and Alberta Netcare
Dr. Sunday Olowu	TELUS Health Solutions Wolf Electronic Medical Records encompassing: PCN participation: Calgary West Central
Dr. T. James	Organization Management and Alberta Netcare
Dr. Tobias Gelber	Chinook Primary Care Network Patient Attachment Initiative and Central Data Repository
Dr. Tyler May	Accuro/Optimed Electronic Medical Records encompassing: Organization Management, Alberta Netcare, and PCN participation: Peace Region
Dr. Uzma Khan	Alberta Netcare and Electronic Medical Records
Dr. Velupillai Velmurugiah	Organization Management encompassing: Paper Patients Records Primary Care Network, Wireless and Physician Netcare Access
Dr. Virinder Singh	Microquest Healthquest Electronic Medical Records local install encompassing: new clinic implementing QSP ASP Hosted Solution, paper records to local install solution Netcare Access and PCN participation: Edmonton Southside
Dr. Wikus Venter	Optimed Accuro Electronic Medical Records ASP implementation: encompassing Alberta Netcare and PCN participation: Calgary West
Dr. Wilfred Alonso	Procedure for Information Handling - Canadian Sleep Consultants and PCN participation: Foothills

CUSTODIAN	PIA TITLE
REGISTERED NURSES	
	12 Alberta Netcare PIAs
Andree McTaggart, RN	Electronic Health Systems Project encompassing: paper community health records to an Electronic Solution - CHIP (Community Health and Immunization Program), Paper Homecare and Diabetes Management records to an Electronic Solutions - CARE (Community Assessment, Response and Empowerment)
Andree McTaggart, RN	Garden River Nursing Station (GRNS) Electronic Health System(s) encompassing: paper community health records to an Electronic Solution-CHIP (Community Health and Immunization Program)
Jessie St. Laurent, RN	Alberta Netcare, Organization Management, and Wireless
Jessie St. Laurent, RN	Fort Chipewyan Health & Wellness Centre Electronic Community Health Information System encompassing: Paper community health records to an electronic Community Health and Immunization Program (CHIP)
Mr. Christopher Wood, RN	SCCOT Electronic Medical Records
Mr. Joseph Redhead, RN, Sturgeon Lake Health Centre	Electronic Medical Records (EMR) PIA encompassing: paper community health records to an Electronic Solution - CHIP (Community Health and Immunization Program)
Mr. Troy Tilley, RN	Saddle Lake Health Care Centre Electronic Health System(s) Electronic Medical Records encompassing: paper community health records to an Electronic Solution: CHIP (Community Health and Immunization Program), Paper Homecare and Diabetes Management Records to an Electronic Solution - CARE (Community Assessment, Response and Empowerment)
Ms. Barb Kilpatrick, RN, Sunchild Health Centre	Sunchild Health Centre Electronic Community Health Information System encompassing: paper community health records to an electronic Community Health and Immunization Program (CHIP) solution
Ms. Beth Woytas, RN	Public Health and Immunization Exchange (PHIX) PIA encompassing: immunization records to an electronic Public Health and Immunization Exchange (PHIX) solution
Ms. Carma Prucyk, RN	Chateh Health Centre Electronic Community Health Information System Project encompassing: paper community health records to an electronic Community Health and Immunization Program (CHIP) solution
Ms. Cherie Willier, RN, Kapawe'no Health Centre	Electronic Community Health Information System PIA encompassing: paper community health records to an electronic Community Health and Immunization Program (CHIP)
Ms. Donna Rowsell, RN	Heart Lake Health Centre Electronic Health Systems Electronic Medical Records encompassing: paper community health records to an Electronic Solution - CHIP (Community Health and Immunization Program)
Ms. Elizabeth Alix McGregor, RN	Little Red River Cree Antion (LRRCN) Electronic Medical Records encompassing: Alberta Netcare access
Ms. Karen Benwell, RN	Alberta Netcare, Wireless, paper community health records to an electronic CHIP solution, and Data Migration

CUSTODIAN	PIA TITLE
Ms. Lori Healy, RN, Blood Tribe Department of Health	Electronic Community Health Information System PIA encompassing: paper community health records to an electronic Community Health and Immunization Program (CHIP) solution
Ms. Nicole Macor, RN	Electronic Community Health Information System
Ms. Sarah Fordham, RN	Maskwacis Health Services Electronic Health System(s)
Ms. Sharla Cadwell, RN	Lubicon Lake Health Centre Electronic Community Health Information System encompassing: paper community health records to an electronic Community Health and Immunization Program (CHIP)
REGIONAL HEALTH AUTHORITIES	
Alberta Health Services	3rd Amendment AHS Data Repository for Reporting (AHSDRR)
	AHS Cross-Enterprise Document Sharing (XDS)
	Alberta Cervical Cancer Screening Program (ACCSP)
	Alberta Colorectal Cancer Screening Program (ACRSP)
	Alberta Health Services Data Respository for Reporting (AHSDRR)
	Alberta Health Services Sleep Centre Enterprise System
	Alberta Provincial Project for Outcome Assessments in Coronary Heart Disease (APPROACH)
	Amendment - AHS Data Repository for Reporting (AHSDRR)
	Amendment Organ Transplant Tracking Record (OTTR)
	Amendment to the AHS Client Registry CR
	Amendment to the Tracking Record (OTTR)
	Amendment to the Transplant Tracking Record (OTTR)
	Amendment: Alberta Cancer Registry Amendment
	Amendment: Cerner Millennium Appointment Reminder System - Computer Talk
	Breast Milk Tracking System Vendor: Clinibase
	Call Centre Anywhere (CCA)
	Cancer Surgery Alberta - SynoptecSystem
	CaseWorks Health Information Management Complex

CUSTODIAN	PIA TITLE
	Cerner Millenium Automated Appointment Reminder System
	Cerner Millenium Automated Appointment Reminder System - Computer Talk
	Chronic Disease Management's Better Choices, Better Health - Online Program
	Correction Health Services - Facility Services Information System
	Dragon Medical Enterprise Network Edition (DMENE)
	Elbow River Healing Lodge
	Electronic Patient Care Record (ePCR)
	eRecords
	eTriage
	Nuance Dragon Medical 360|eScription
	Patient Panel Data Analysis - A Data Matching Project between AHS (Chinook Health) and Family Practice Physicians and Alberta Health Amendment #1
	Provincial Alberta Perinatal Health Program - PeriLink AB
	Pyxis Automated Dispensing System
	Review PIA: Cube Cardiac MRI Reporting Solution
	St. Jude Medical Merlin.net Patient Care Network
SUBSIDIARY HEALTH CORPORATIONS	
DynaLIFE Dx Diagnostic Laboratory Services	Appointment Booking Wait Time Management (Booking System)
Calgary Laboratory Services Ltd.	Cellavision

CUSTODIAN	PIA TITLE
PRIMARY CARE NETWORKS	
Calgary Foothills Primary Care Network (PCN)	Migration of CFPCN E-mail Server and Communications Platform to Microsoft Office 365 & Microsoft Lync
Calgary Mosaic Primary Care Network (PCN)	Transfer of Patient Information
Chinook Primary Care Network	Patient Attachment Initiative and Central Data Repository
Cold Lake Primary Care Network	Cold Lake Primary Care Network - Satellite Clinic Vendor: TELUS EMR
Drayton Valley PCN	Electronic Medical Records to: DVPCN
Edmonton North Primary Care Network	Med Access Electronic Medical Records and Call Remonder System (Cliniconex) Vendor: Med Access encompassing: Appointment Reminder System (Cliniconex) POSP Physician Netcare Access
Edmonton West Primary Care Network	Addendum Edmonton West PCN
Grande Prairie Primary Care Network (PCN)	Organization Management and Participation with Grande Prairie Primary Care Network After - Hours Clinic, Chronic Pain Management Program, Care Coordination, Direct Care Provision and Alberta Netcare
Highland Primary Care Network	Organization Management and OSCAR Electronic Medical Records encompassing Alberta Netcare
Highland Primary Care Network	Organization Management and OSCAR Electronic Medical Records encompassing Alberta Netcare
Hinton Primary Care Network	Organizational Management and Alberta Netcare
Wood Buffalo Primary Care Network	TELUS Health Solution Wolf Electronic Medical Records encompassing: Data Migration, Wireless, QSP local install to QSP hosted Electronic Medical Record, Netcare Access and PCN participation: Wood Buffalo
ORGANIZATION	**PIA TITLE**
PROFESSIONAL, SCIENTIFIC AND TECHNICAL SERVICES	
Reach Edmonton Council for Safe Communities	24/7 Edmonton Outreach Worker Application
INSURANCE	
Allstate Insurance Company of Canada	Allstate Insurance Company of Canada usage-based insurance (UBI) Program

www.oipc.ab.ca